



U.S. Department of Justice
Federal Bureau of Investigation

Office of Public and Congressional Affairs

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-09-2005 BY 65179DMH/lr2 Ca #05-CV-0845

Director 5/20/04
STC Hearing

DATE: 12-03-2005
CLASSIFIED BY 65179/DMH/DD 05-CV-0845
REASON: 1.4 (C)
DECLASSIFY ON: 12-03-2030

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~Secret~~

QUESTIONS FOR THE RECORD FROM DIRECTOR'S 5/20/04 SENATE
HEARING

NSLB RESPONSES

28. OGC. During the hearing, Senator Grassley asked you about the retroactive classification of information provided by the FBI to Committee staff related to a whistleblower who previously worked for the FBI translation program. I share Senator Grassley's concern that this order is unrealistic. A great deal of information regarding the whistleblower's claims, including the FBI's corroboration of many of the problems she raised, has been in the public record for more than two years. I appreciated your statement that the retroactive classification order was not intended to place a gag on Congress. However, the notice received by staff members of the Judiciary Committee was very vague, referring only to "some" information conveyed in the briefings. If state secrets are truly implicated by something that was said in an unclassified briefing two years ago, the FBI should provide very specific instructions to current and former staff on what information must be kept secret. Will you instruct your staff to provide more specific information to relevant staff about what, exactly, from the 2002 briefings is classified and what is not?

b5

33. OGC. You testified that, prior to the PATRIOT Act, "if a court-ordered criminal wiretap turned up intelligence information, FBI agents working on the criminal case could not share that information with agents working on the intelligence case." Please state specifically what law or laws prevented such information-sharing prior to PATRIOT, and whether a court could authorize such information-sharing, regardless of any such law or laws?

Response: Prior to the changes brought about by the Patriot Act, Title 18 Section 2517 was interpreted to solely authorize the sharing of intercepted wire, oral, or electronic

~~SECRET~~

~~SECRET~~

communications for criminal law enforcement purposes without the need to obtain a court order. Sharing intercepted information for foreign intelligence purpose required a court order and, based upon the statutory language, it was unclear whether a judge would sign an order. The changes to the Patriot Act clearly allow the sharing of foreign intelligence information developed during a court-ordered criminal wiretap with the agents working intelligence cases.

34. OGC. You further testified that, prior to the PATRIOT Act, "information could not be shared from an intelligence investigation to a criminal investigation." Please state specifically what law or laws prevented such information-sharing prior to PATRIOT?

Response: Prior to the Patriot Act, there were procedures for sharing information between intelligence investigators and criminal agents and prosecutors, but they were difficult, burdensome and usually resulted in less than fulsome sharing. For example, the FISA statute was interpreted to require a "primary purpose" of gathering intelligence in order to secure a FISA Court order. Because of this interpretation of the FISA statute, the Department of Justice and the FISA Court required that certain procedures be followed in order to share intelligence with criminal investigators and prosecutors.

b5

For additional information, see the answer to question 35.

35. OGC. In his statement to the 9/11 Commission, the Attorney General blamed the creation of the so-called "wall" between criminal investigators and intelligence agents on a 1995 memorandum authored by a senior official in the Reno Justice Department, now a member of the 9/11 Commission.

a. Do you agree that the architecture of the wall was in place long before 1995, having its genesis in established legal doctrine dating from 1980? If not, how do you explain the extensive discussion of this issue in the one and only reported opinion of the FISA Court of Review, decided on November 18, 2002?

~~SECRET~~

~~SECRET~~

[REDACTED]

b5

[REDACTED]

b5

[REDACTED]

b5

[REDACTED]

b5

~~SECRET~~

~~SECRET~~

b5

How did the FBI handle information-sharing between criminal investigators and intelligence agents before 1995?

b5

b. Do you agree that the Gorelick memo established proactive guidelines amidst a critically important terrorism prosecution to *facilitate* information sharing.

b5

~~SECRET~~

~~SECRET~~

possible. [REDACTED]
[REDACTED]

b5 [REDACTED] In addition, as the Acting Deputy Attorney General explained in his November 20, 2003 Memorandum to the Inspector General in response to the Inspector General's report, the FBI will work with DHS to establish criteria for future investigations (the specific criteria will depend on the nature of the national emergency). For example, an effort is underway to prepare an MOU between DHS and DOJ regarding criteria and procedures for determining alien detainees of national security interest. In addition, the creation of TSC and TTIC will greatly improve the FBI's ability to gather information concerning aliens of national security interest and work with the appropriate federal agencies to determine the best means of averting any national security threat, whether through criminal or immigration proceedings. Other initiatives, such as the Foreign Terrorist Tracking Task Force and the National Joint Terrorism Task Force have assisted in permitting better information flow with our law enforcement counterparts and will improve the handling of such cases. [REDACTED]
[REDACTED]

82. OGC. Title 18 Section 3103a, as amended by Section 213 of the USA-Patriot Act (P.L. 107- 56), provides authority for delaying notice of the execution of search warrants. The following question pertains to the use of the authority provided in this section in investigations or prosecutions related to terrorism during the period of time from September 11, 2001 to the present.

a. In how many such cases has the authorities to delay notification been used?

b. In how many such cases has the authority added by Section 213(b)(1), which allows a delay where "the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result" been used? Please describe the circumstances in each of these cases.

c. In how many such cases has the authority set forth in 18 U.S.C. 2705(E), which provides for delay in cases which would "otherwise seriously jeopardize an investigation or unduly

~~SECRET~~

~~SECRET~~

[delay] a trial" been used? Please describe the circumstances in each of these cases?

b5

84. Sections 203(b) and 203(d) of the USA-Patriot Act provide specific authority for the provision of intelligence information acquired in the course of a criminal investigation to elements of the Intelligence Community. Section 901 of the same act makes such disclosure in most cases mandatory. The following questions pertain to the implementation of these sections.

a. OGC. Section 203(c) of the USA-Patriot Act requires the Attorney General to "establish procedures for the disclosure for the disclosure of information" as provided for in Section 203. Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

Response to Q84 a: On September 23, 2002, the Attorney General promulgated guidelines that established the procedures for disclosure of information under Section 203 of the Patriot Act. A copy of the guidelines is attached. The Office of the General Counsel issued an EC advising all Divisions of the procedures. A copy of the EC is attached.

b. OGC. Section 203(b) specifically provides authority "to share electronic, wire, and oral interception information" where such information is foreign intelligence information. What is the method for disseminating such information to the Intelligence Community?

Response to Q84 b: The FBI disseminates intelligence information via Intelligence Information Reports (IIRs). With regard to 203 (b) material, the FBI does not track or keep a central database as to how many reports, if any, contain 203 (b) material.

b5

~~SECRET~~

~~SECRET~~

b5

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203 (b) material?

The FBI disseminates raw intelligence via the IIR. If 203 (b) material is disseminated it would be through this mechanism. The FBI does not keep a database as to whether 203 (b) material is contained with any disseminated IIR.

(1) If so, how many such reports have been issued?

Response: The FBI has no central database readily to determine the quantity of 203 (b) material disseminations through the aforementioned methods.

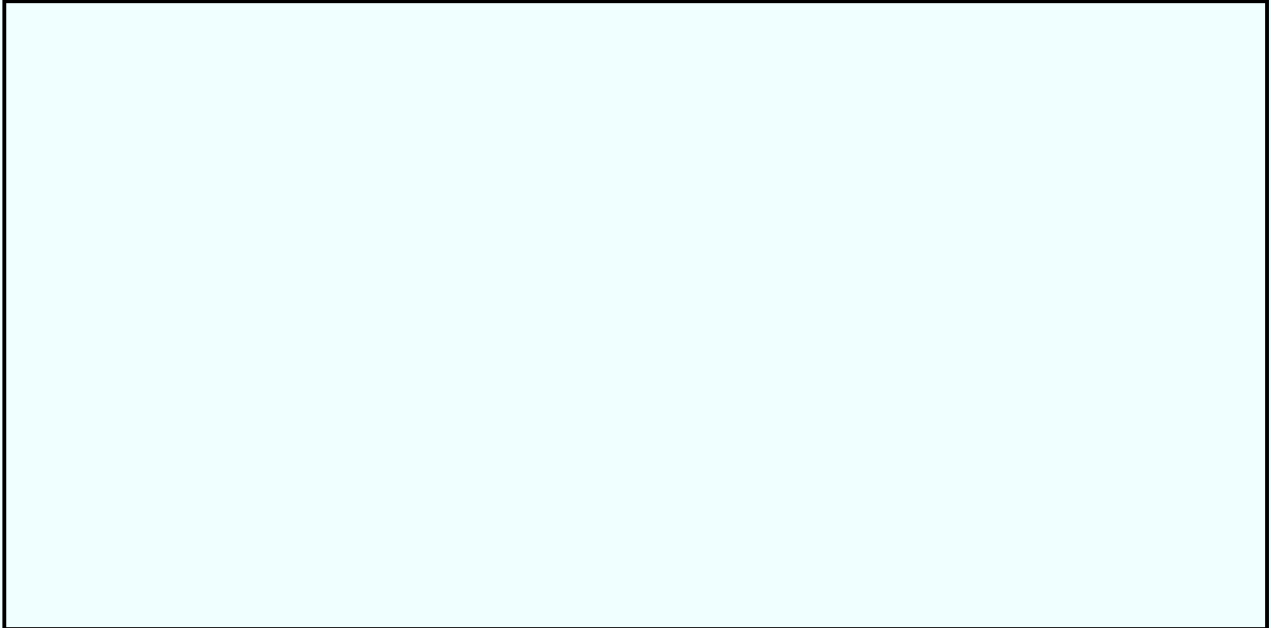
During the period August, 2002 (the beginning time-frame in which statistical data was collected), through August, 2004, the Counterterrorism Division has disseminated approximately 3860 IIRs. Of that total, 240 of those IIRs contain FISA-derived intelligence. The remaining number of IIRs are derived from various sources and methods which may or may not include Title 3

~~SECRET~~

~~SECRET~~

derived information. In addition, other divisions besides the Counterterrorism Division disseminate IIRs.

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?



b5

c. OGC. Section 203(d), the so-called "catch-all" provision, provides a general authority to share foreign intelligence information with the Intelligence Community. What is the method for disseminating such information to the Intelligence Community?

Response: The FBI disseminates raw intelligence via the IIR. If 203 (d) material is disseminated it would be through this mechanism. The FBI does not keep a database as to whether 203 (d) material is contained in any disseminated IIR.



b5

~~SECRET~~

~~SECRET~~

b5

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(d) material?

Response: Dissemination of Electronic, Wire, and Oral Interception Information to the IC derived through standard criminal procedures may be effected electronically through IIRs, TM, Intelligence Assessments, Intelligence Bulletins. However, dissemination of this intelligence information also may be transacted through the exchange of FBI Letterhead Memoranda (LHMs) among relevant IC members.

(1) If so, how many such reports have been issued?

Response: The FBI has no central database to determine the quantity of 203(d) material disseminations through the aforementioned methods.

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

b5

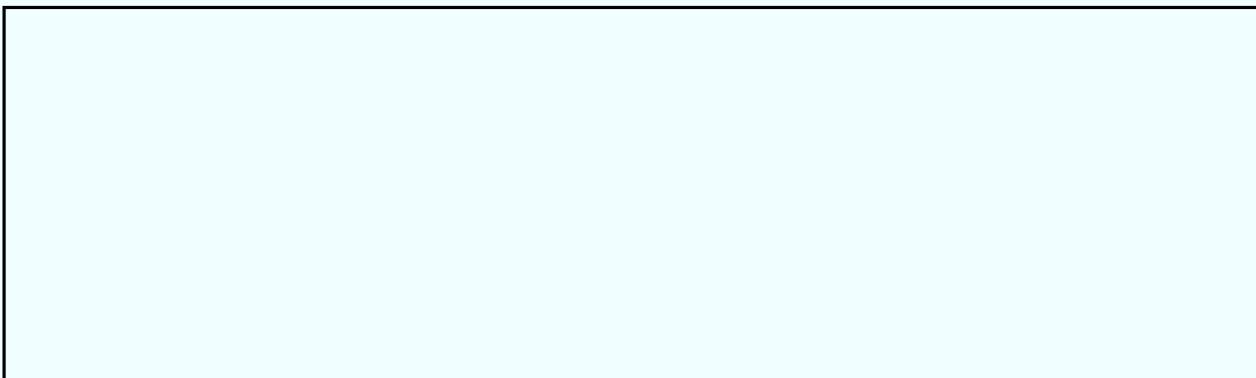
~~SECRET~~

~~SECRET~~



b5

d. OGC. Section 905(c) of the USA-Patriot Act requires the Attorney General to "develop procedures for the administration of this section. . . ." Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

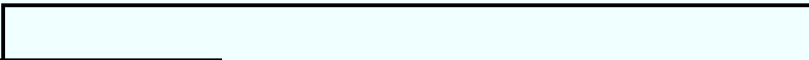


b5


e. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 203 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

f. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:



b5

 OGC strongly believes that Section 203 (b) and (d) should not be allowed to expire on December 31, 2005. The changes brought about by the Patriot Act have significantly increased the ability of the FBI to share information.

85. Sections 206 of the USA-Patriot Act, the so-called "roving wiretap" provision, permits the issuance of a FISA warrant in cases where the subject will use multiple communication

~~SECRET~~

~~SECRET~~

facilities. This question pertains to the implementation of this section during the time period since the passage of the USA-Patriot Act, October 26, 2001.

Response:

a. How often has this authority been used, and with what success?

b5

b. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to the FISA?

Response: FBI intelligence products are an important vehicle for the dissemination of both FISA-derived and non-FISA foreign intelligence information, but not the only one.

b5

More specifically, the FBI shares many forms of foreign intelligence with other members of the Intelligence Community.

b5

through direct classified and unclassified dissemination and through websites on classified Intelligence Community networks. The FBI also shares intelligence with representatives of other elements of the Intelligence Community who participate in Joint Terrorism Task Forces (JTTFs) in the United States or with whom the FBI collaborates in activities abroad. FBI intelligence products shared with the Intelligence Community include Intelligence Information Reports (IIRs), Intelligence Assessments, and Intelligence Bulletins.

~~SECRET~~

~~SECRET~~

The FBI also disseminates intelligence information through Law Enforcement Online (LEO), a virtual private network that reaches federal, state, and law enforcement agencies at the Sensitive But Unclassified (SBU) level. LEO makes finished FBI intelligence products available, including Intelligence Assessments resulting from analysis of criminal, cyber, and terrorism intelligence, [REDACTED]

b5

[REDACTED] Intelligence Information Reports also are available on LEO at the Law Enforcement Sensitive classification level. The FBI also recently posted the requirements document on LEO, which provided state and local law enforcement a shared view of the terrorist threat and the information needed in every priority area.

(i) If so, how many such reports have been issued?

Response: In the past two years the FBI's Counterterrorism Division's Terrorism Reports and Requirements Section has disseminated 76 intelligence information reports (IIRs) containing information derived from FISA-authorized surveillance and/or search. (Statistics are not maintained in such a way that would enable us to say whether any of the FISA-derived information in the reports was obtained using "roving authority.") Other FBI Divisions have also issued reports containing FISA-derived information. For example, the Cyber Division has written a total of 24 electronic information reports containing FISA-derived information.

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response: The Office of Intelligence promulgated the FBI's Intelligence Information Report Handbook on 9 July. The Handbook establishes the first comprehensive FBI-wide guide for the format and content of raw intelligence reports. The Office of Intelligence is working to develop evaluation guidelines based, in part, on the criteria established in the Handbook for the types of information to be reported and shared with our law enforcement and intelligence community partners, [REDACTED]

b5

In addition, the FBI's Inspection Division has established evaluation criteria for the value of human source reporting, [REDACTED]
[REDACTED] access and responsiveness to local FBI field office,

b5

~~SECRET~~

~~SECRET~~

FBI program and national intelligence requirements . The Office of Intelligence is developing guidelines to use this same criteria as a means of evaluating the value of raw intelligence. Initial discussions on this issue have been held with representatives from the Counterintelligence, Counterterrorism, Criminal and Cyber Divisions. The results of these discussions are being incorporated into evaluation guidelines.

c. Some have read this section as providing for surveillance in cases where neither the identity of the subject or the facility to be used is known -- in effect, allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversation of an unknown person. Is this the reading of the statute being adopted by the Federal Bureau of Investigation and the Department of Justice? If not, please provide your interpretation of this authority.

Response: No, the FBI does not interpret the statute as allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversations of an unknown person. In order to make a showing of probable cause, the FISA statute requires a statement of the facts and circumstances relied upon by the applicant for surveillance to justify the belief that: (1) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and, (2) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. Thus, the FISA statute does not permit coverage to be authorized, with or without the "roving wiretap" provision, to allow for surveillance against all persons in a particular geographic area. The FBI has interpreted the "roving" authority as permitting the FBI to request that the Foreign Intelligence Surveillance Court issue a "generic" secondary order, along with specified orders, for a specifically identified FISA target, that the FBI could serve in the future on the unknown (at the time the order is issued) cell phone carrier, Internet service provider, or other communications provider, if the target rapidly switches from one provider to another. The roving wiretap order still requires that a federal law enforcement agent swear in a detailed affidavit to facts establishing probable cause, and still requires a court to make a finding of probable cause before issuing the order. The roving order has the additional requirement of a judge's approval to monitor more than one telephone. But now, each time a target changes his cellular telephone, instead of going through the lengthy application process, government agents can use the same order to monitor the

~~SECRET~~

~~SECRET~~

target. This will allow the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the Court for a new secondary order. The FBI views this as a vital and necessary tool to counter certain targets who engage in such actions as a deliberate means of evading surveillance.

(i) Have any briefs been filed with the Foreign Intelligence Surveillance Court on this subject? If so, please provide copies of such briefs to the Committee.

Response: The FBI has filed no such briefs on this subject.

d. Inspection Division

e. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response: No, we request only that the provision be preserved.

86. Section 207 of the USA-Patriot Act extends the time limits provided in the FISA which govern surveillance against agents of a foreign power.

a. Has the Federal Bureau of Investigation or the Department of Justice conducted any review to determine whether, and if so, how many, personnel resources have been saved by this provision? If so, please provide the results to the Committee.

b5

b. Have there been any cases where, after the passage of the now-extended deadlines it was determined, either by the Department of Justice, the Federal Bureau of Investigation or the Foreign Intelligence Surveillance Court, that surveillance should have been terminated at an earlier point because of the absence of a legally required predicate.

Response: None of which the FBI is aware.

~~SECRET~~

~~SECRET~~

c. Inspection Division

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response: None at this time.

89. Section 214 of the USA-Patriot Act permits the use of FISA pen register/trap & trace orders with respect to electronic communications, and eliminates the requirement that such use be only in the context of a terrorist or espionage investigation. This question pertains to application of this provision since its passage, and to all instances, not only terrorism investigations.

a. OGC. In how many cases has this authority been used?

(i) How many of such cases were terrorism-related?

b5

b. OGC. Of the cases in which such authority was used, in how many was a subsequent application for a full surveillance order made pursuant to the FISA, or Chapter 19 of Title 18?

Response: OGC does not have a way to determine how many pen registers evolved into full FISA's.

c. Inspection Division. Has the Intelligence Community, Department of Justice, or Federal Bureau of Investigation developed regulations or directives defining the meaning of non-content communications? If such regulations or directives have been issued, please provide copies to the Committee.

d. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation

~~SECRET~~

~~SECRET~~

disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response: Please see answer to Question 85.

90. Section 215 of the USA-Patriot act authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application of this provision since its inception.

a. OGC. How many times has this authority been used, and with what success?

b. OGC. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.

c. OGC. In your testimony you compared this provision with existing authority in the criminal context, noting that records such as library records are subject to a grand jury subpoena. However, in criminal cases the propriety and lawfulness of subpoenae are to some extent tested in the adversary process of a trial - how, in the context of the FISA, does such a check occur?

d. OGC. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

(i) With respect to the potential applicability of this section to libraries and bookstores, there has been some concern that the mere prospect of use of the statute has a "chilling effect" on the use of these facilities. Can this chilling effect be minimized, if not eliminated, by incorporating a higher threshold for use in the limited context of libraries and bookstores? If not, why not?

~~SECRET~~

~~SECRET~~

e. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

f. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

g. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

[REDACTED]
[REDACTED]
[REDACTED] (S)

b1

[REDACTED]
[REDACTED] (S)

b2

b7E

b5

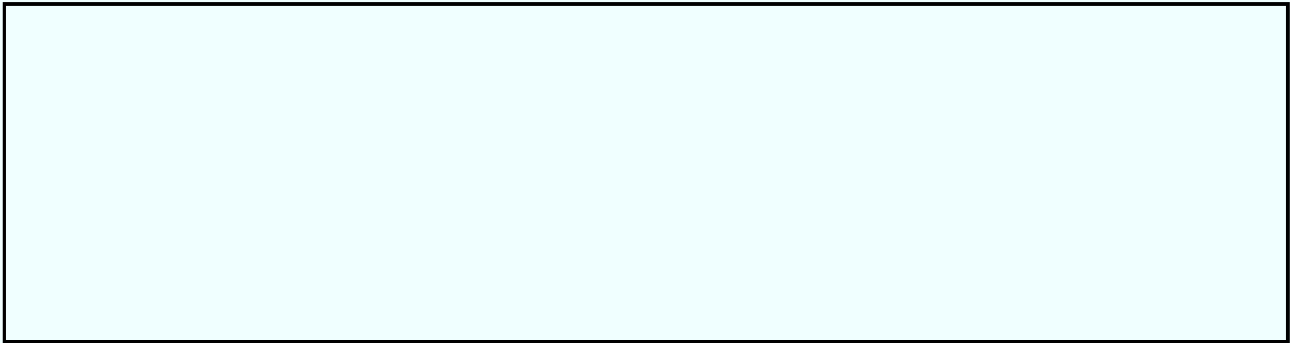
[REDACTED]
[REDACTED] (U)

[REDACTED]

b5

~~SECRET~~

~~SECRET~~



b5



b2

b7E

b5



. (U)

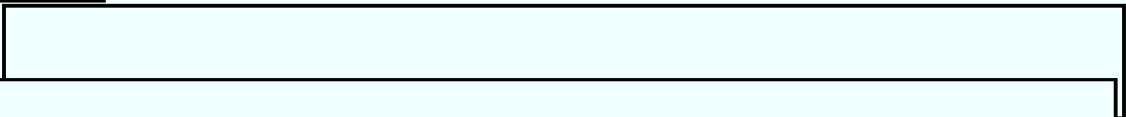


b5



(U)

d.



b1

b2

b7E

b5

b5

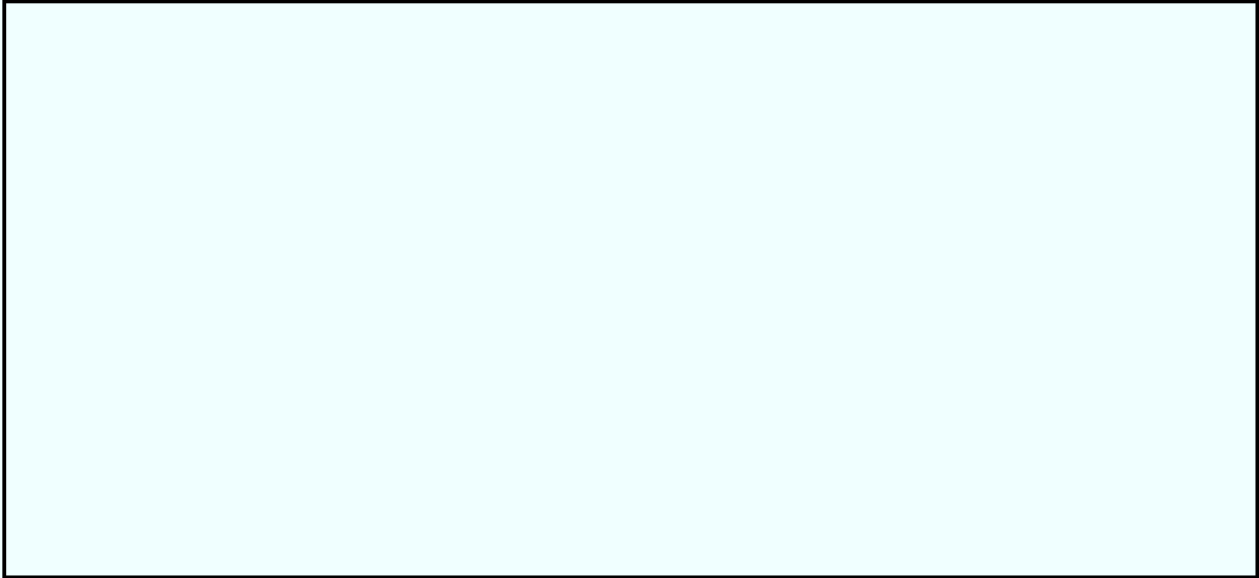
~~SECRET~~

~~SECRET~~

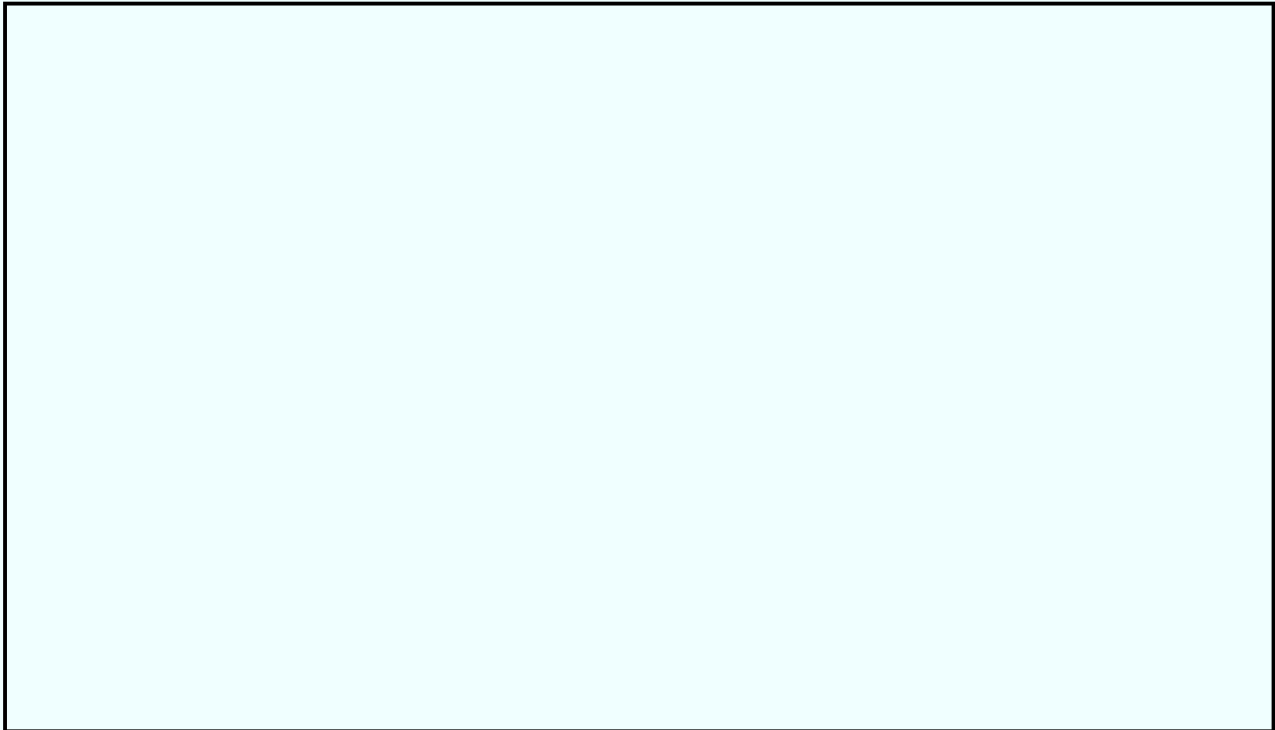


(S)

b1



b5



b5

~~SECRET~~

~~SECRET~~

[REDACTED]

[REDACTED]

b5

[REDACTED]

[REDACTED]

b5

[REDACTED]

92. Section 218 of the USA-Patriot Act created the so-called "significant purpose" test for applications pursuant the FISA, clarifying the law to recognize that in many cases such surveillance may implicate both a law enforcement and an intelligence interest. This question pertains to the implementation of this provision since its passage.

a. OGC. Please provide the Committee with specific examples, in unclassified form if possible, of cases in which both law enforcement and intelligence interests were "significant."

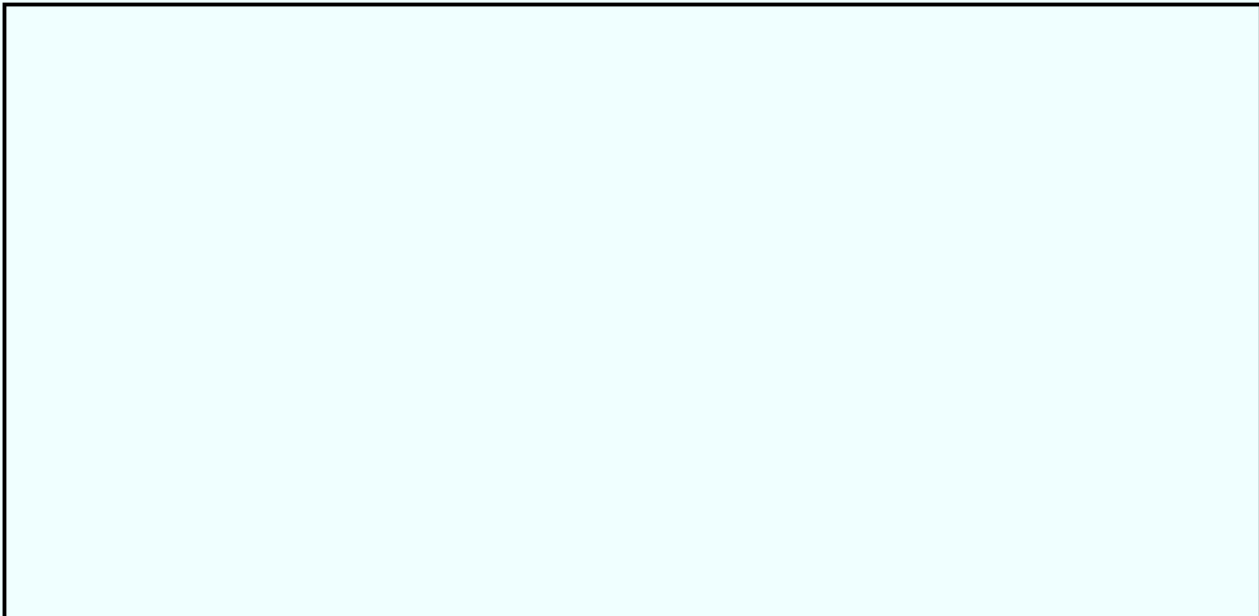
b. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 218 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

c. OGC. Based upon the application of this provision of law

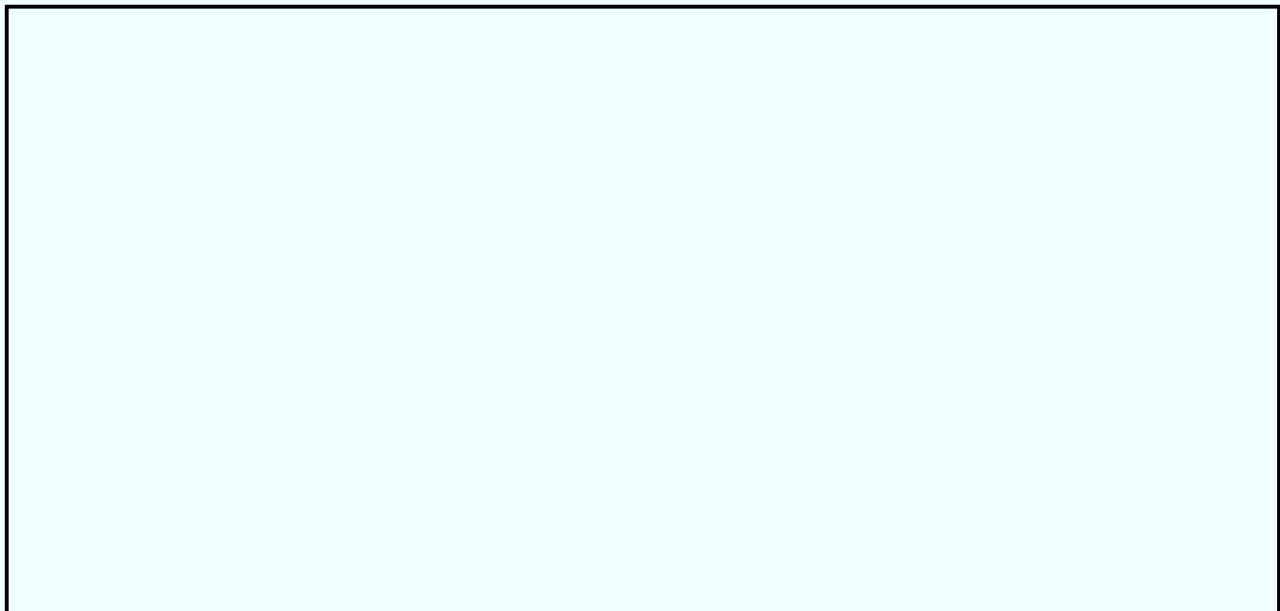
~~SECRET~~

~~SECRET~~

during the period since its passage, are there changes to this statute which the Congress should consider?



b5



b5



(S)

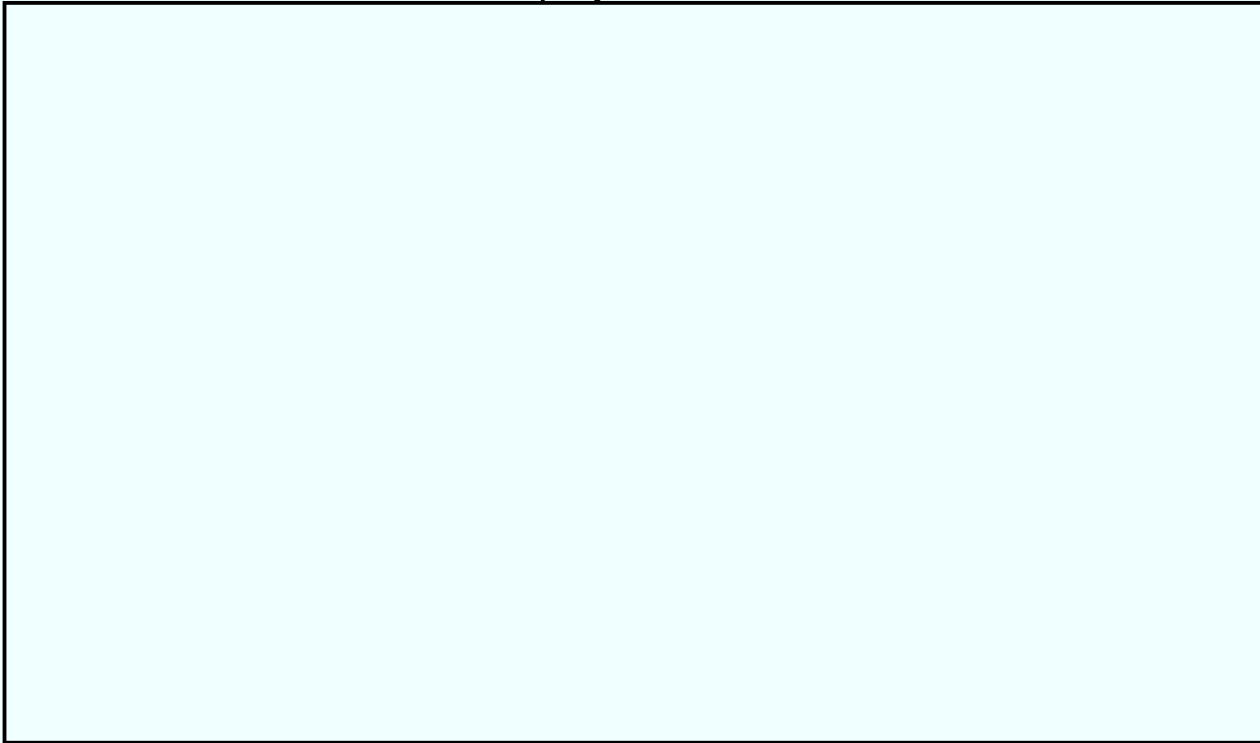
(S)



b1
b5
b7A

~~SECRET~~

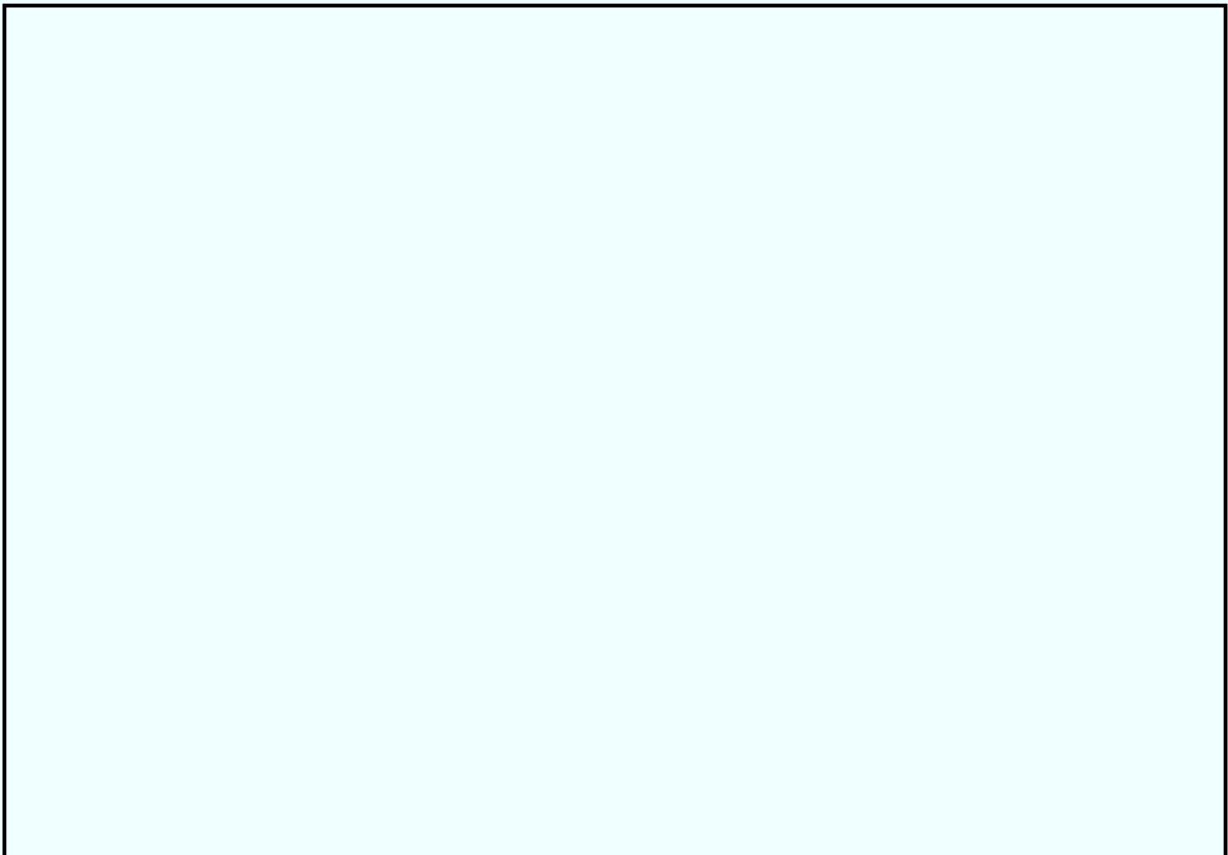
~~SECRET~~



(S)

b1
b5
b7A

(S)



b5
b7A
b6
b7C

~~SECRET~~

~~SECRET~~

[Redacted]

[Redacted]

b5
b7A

[Redacted]

(S)

b1
b5
b7A

[Redacted]

(S)

[Redacted]

[Redacted]

[Redacted]

b5

[Redacted]

b5
b7A

[Redacted]

b6
b7C

[Redacted]

~~SECRET~~

~~SECRET~~

b5
b6
b7C

c. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which Congress should consider?

b5

101 d. OGC. According to court records, no criminal charges were ever filed against Mayfield. Instead, he was detained as a material witness. Why was Mayfield held as a material witness and not charged with any criminal conduct?

b6
b7C
b5

100 e. CTD (in coordination with OGC). Mayfield has stated that he

~~SECRET~~

~~SECRET~~

believes that his home was secretly searched before he was declared a material witness and detained. Prior to, or during his detention, was the Mayfield residence or office searched pursuant to a warrant under the Foreign Intelligence Surveillance Act (FISA) or a delayed notification search warrant? If the latter, please indicate (a) the basis for seeking delayed notice of the search warrant and (b) the time period requested and granted for delaying notice

b1
b5
b6
b7C

[REDACTED]

(S)

103. OGC. In September 2003, the U.S. Department of Justice disclosed that it had not yet used section 215 of the USA PATRIOT Act. On March 9, 2004, I sent a letter to the Attorney General asking him to clarify whether section 215 has been used since September 18, 2003. (Copy of letter attached.)

a. Please indicate whether section 215 has been used since September 18, 2003.

b. If section 215 has been used, please describe how it has been used. How many U.S. persons and non-U.S. persons were targets of the investigation? Was the section 215 order served on a library, newsroom, or other First Amendment sensitive place? Was the product of the search used in a criminal prosecution?

b1
b5
b6
b7C

[REDACTED]

[REDACTED]

(S)

b

[REDACTED]

[REDACTED]

(S)

~~SECRET~~

b. Section 203(b) specifically provides authority "to share electronic, wire, and oral interception information" where such information is foreign intelligence information. What is the method for disseminating such information to the Intelligence Community?

Response:

Electronic, wire, and oral interception information derived through standard criminal procedures may be disseminated to the IC through any means appropriate to the circumstances, including Intelligence Information Reports (IIRs), Teletype Memoranda, Intelligence Assessments, Intelligence Bulletins, and FBI Letterhead Memoranda.

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(b) material?

Response:

The FBI disseminates intelligence information via the IIR, which is an electronic communication format widely accepted in the IC as the standard intelligence dissemination vehicle. IIRs consist of raw intelligence (intelligence which has not been finally evaluated) and associated clarifying information that puts the raw intelligence into context. IIRs are drafted and prepared by the FBI's cadre of Intelligence Analysts/Reports Officers. Before FBI intelligence is disseminated, it is analyzed and sanitized to protect intelligence sources and methods and, if applicable, United States persons and entities that may be compromised or negatively impacted if left unprotected. FBI Program Managers and Intelligence Analysts concurrently identify intelligence that is consistent with IC intelligence requirements and interests.

(1) If so, how many such reports have been issued?

Response:

Although CTD is not the only FBI producer of IIRs, that Division reports that, during the period from August 2002 (when statistical data was first collected) through August 2004, CTD has disseminated approximately 3,860 IIRs [REDACTED]

b2

b7E

[REDACTED] The remaining IIRs have been

derived from various sources and methods which may or may not include Title III information.

The FBI does not track or maintain a central database with respect to the number of IIRs containing 203(b) material, if any.

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

Determinations to disseminate electronic, wire, and oral intercept information are made with input from Operational Program Managers, Intelligence Analysts, the National Security Law Branch, and, when appropriate, DOJ. This evaluation considers the value of the information not only to the IC but also, depending on the proposed use, context, and nature of any threat-related information, to federal, state, and local law enforcement entities and, when authorized by DOJ, to foreign intelligence services and foreign law enforcement agencies.

The quality and value of IIRs are evaluated through several means. On each IIR, the Reports Officer provides information by which the customers can contact the Reports Officer directly. The quality and relevance of the reporting is also reflected by the submission of additional collection requirements; IC members often forward formal Requests for Information (RFIs) with respect to information that has been protected (not provided) in the IIR, such as U.S. Person information. Such RFIs provide an excellent indication of IC interest in FBI reporting. In addition, IC members often provide feedback with respect to specific IIRs directly to the FBI Intelligence Analysts/Reports Officers who author the reports. The FBI's OI also often receives evaluations of FBI reporting, and is working to establish a formal IIR evaluation mechanism by which recipients can rate or provide feedback on FBI intelligence reporting.

c. Section 203(d), the so-called "catch-all" provision, provides a general authority to share foreign intelligence information with the Intelligence Community. What is the method for disseminating such information to the Intelligence Community?

Response:

The FBI shares foreign intelligence information, as defined in Section 203(d)(2), with the IC through several conduits. Dissemination can be through direct classified and unclassified IIRs, Intelligence Assessments, Intelligence Bulletins,

Teletype Memoranda, or IC web sites on classified networks. The FBI also shares intelligence information through the FBI's Joint Terrorism Task Forces (JTTFs), which include members of the IC and operate in 100 locations across the United States. Unclassified but "law enforcement sensitive" intelligence information is also disseminated to federal, state, and local law enforcement intelligence components through Law Enforcement Online (LEO), a computer network which provides finished intelligence products, assessments, and bulletins on significant developments and trends.

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(d) material?

Response:

Electronic, wire, and oral interception information derived through standard criminal procedures may be disseminated to the IC through any appropriate means, including IIRs, Teletype Memoranda, Intelligence Assessments, Intelligence Bulletins, and FBI Letterhead Memoranda.

(1) If so, how many such reports have been issued?

Response:

While the FBI does not track or maintain a central database with respect to the number of IIRs containing 203(d) material, if any, the July 2004 DOJ "Report From the Field: The USA PATRIOT Act at Work" indicates that DOJ has made disclosures of vital information to the intelligence community and other federal officials under section 203 on many occasions. For instance, such disclosures have been used to support the revocation of visas of suspected terrorists and prevent their reentry into the United States, to track terrorists' funding sources, and to identify terrorist operatives overseas.

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

There are various means by which IIRs are evaluated. Members of the IC often provide feedback assessing the quality and value of specific IIRs directly to the FBI Intelligence Analysts/Reports Officers who author the reports. On each IIR, the Reports Officers identify the means by which customers can contact them directly. IC members assess the quality and relevance of the reporting, and submit additional collection requirements when appropriate. Often, IC members forward formal Requests for Information (RFIs), which can provide an excellent indication of IC interest in FBI reporting. The FBI's OI also receives evaluations of FBI reporting. The OI is working to establish a formal IIR evaluation mechanism by which recipients can rate or provide feedback on FBI intelligence reporting.

d. Section 905(c) of the USA-Patriot Act requires the Attorney General to "develop procedures for the administration of this section. . . ." Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

Response:

Pursuant to Section 905, DOJ developed the Attorney General's Guidelines Regarding Information Sharing under the USA PATRIOT Act. These guidelines are available on the website of DOJ's Office of Legal Policy (OLP) (www.usdoj.gov/olp). Additionally, among other Department materials relating to information sharing are the following:

- The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, Part VII.B. (10/31/03) (concerned in part with information sharing with intelligence agencies) – Portions of these guidelines are classified, but Part VII.B., relating to information sharing, is unclassified and appears without deletions on OLP's website.
- Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing (3/4/03).
- Memorandum from the Attorney General entitled, "Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation" (9/23/02) – Available on OLP's website.

- Memorandum from the Attorney General entitled, "Coordination of Information Relating to Terrorism" (4/11/02) (concerned in part with information sharing with other Federal agencies) – Available on OLP's website.
- Memorandum from the Attorney General entitled, "Prevention of Acts Threatening Public Safety and National Security" (11/8/01) (concerned in part with information sharing with other Federal agencies) – Available on OLP's website.
- Memorandum from the Attorney General entitled, "Disseminating Information to Enhance Public Safety and National Security" (Sept. 21, 2001) (concerned in part with information sharing with other Federal agencies) – Available on OLP's website.

e. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 203 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the [REDACTED] [REDACTED] none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

b6
b7C

f. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

b5

85. Section[] 206 of the USA-Patriot Act, the so-called "roving wiretap" provision, permits the issuance of a FISA warrant in cases where the subject will use multiple communication facilities. This question pertains [to] the implementation of this section during the time period since the passage of the USA-Patriot Act, October 26, 2001.

a. How often has this authority been used, and with what success?

Response:

The response to this question is classified and is, therefore, provided separately.

b. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to the FISA?

Response:

FBI intelligence products are an important vehicle for the dissemination of both FISA-derived and non-FISA foreign intelligence information, but not the only one. The FBI shares many forms of foreign intelligence with other members of the IC through direct classified and unclassified disseminations, through web sites on classified IC networks, through its participation in Joint Terrorism Task Forces (JTTFs), and through its collaboration in activities abroad.

FBI intelligence products shared with the IC include IIRs, Intelligence Assessments, and Intelligence Bulletins. The FBI also disseminates intelligence information through LEO, a virtual private network that reaches federal, state, and local law enforcement agencies at the Sensitive But Unclassified (SBU) level. LEO makes available to all users finished FBI intelligence products, including intelligence assessments resulting from the analysis of criminal, cyber, and terrorism intelligence, finished intelligence concerning significant developments or trends, and IIRs that are available at the SBU level. In addition, the FBI recently posted the requirements document on LEO, providing to state and local law enforcement a shared view of the terrorist threat and the information needed in every priority area.

(i) If so, how many such reports have been issued?

Response:

In the past two years, CTD's Terrorism Reports and Requirements Section has disseminated 76 IIRS containing information derived from FISA-authorized surveillance and/or searches. (Statistics are not maintained in a way that would enable us to advise whether any of the FISA-derived information in the reports was obtained using roving wiretap authority.) Other FBI Divisions have also issued reports containing FISA-derived information. For example [REDACTED]

b2

b7E

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

The OI promulgated the FBI's Intelligence Information Report Handbook on 7/9/04. The Handbook establishes the first comprehensive FBI-wide guide for the format and content of raw intelligence reports. The OI is also working to develop evaluation guidelines based, in part, on the criteria established in the Handbook for the types of information to be reported and shared with law enforcement and IC partners.

In addition, the FBI's Inspection Division has established criteria for assessing: the value of human source reporting; access to and the responsiveness of local FBI field offices; and FBI program and national intelligence requirements. The OI is developing guidelines for using these same criteria to assess the value of raw intelligence. Initial discussions on this issue have been held with the CI, CT, Criminal, and Cyber Divisions, and the results of these discussions are being incorporated into evaluation guidelines.

c. Some have read this section as providing for surveillance in cases where neither the identity of the subject or the facility to be used is known -- in effect, allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversation of an unknown person. Is this the reading of the statute being adopted by the Federal Bureau of Investigation and the Department of Justice? If not, please provide your interpretation of this authority.

Response:

No, DOJ does not interpret the statute as allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept

the conversations of an unknown person. In order to make a showing of probable cause, the FISA statute requires a statement of the facts and circumstances relied upon by the applicant for surveillance to justify the belief that: (1) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and, (2) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. Thus, the FISA statute does not permit coverage to be authorized, with or without the "roving wiretap" provision, for surveillance of all persons in a particular geographic area. The FBI has interpreted the "roving" authority as permitting the FBI to request that the FISA Court issue, along with the primary order, a "generic" secondary order with respect to a specifically identified FISA target that the FBI can serve in the future on a currently unknown cell phone carrier, Internet service provider, or other communications provider, if the target rapidly switches from one provider to another. The roving wiretap order still requires that a federal law enforcement agent swear, in a detailed affidavit, to facts establishing probable cause, and still requires a court to make a finding of probable cause before issuing the order. While the roving order carries the additional requirement of a judge's approval to monitor more than one telephone, it permits government agents to continue to monitor the target, even if the target changes to a different cellular telephone, rather than first going through the lengthy application process to monitor that new phone. This will allow the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the FISA Court for a new secondary order. The FBI views this as a vital tool to follow targets who change cell phone providers or other communication channels as a deliberate means of evading surveillance.

(i) Have any briefs been filed with the Foreign Intelligence Surveillance Court on this subject? If so, please provide copies of such briefs to the Committee.

Response:

The FBI does not file briefs with the FISA Court. While OIPR files briefs with that Court on behalf of DOJ and the government, it has filed no such briefs on this subject.

d. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 206 of the USA-Patriot Act? If so, please describe the nature and disposition of such a complaint.

Response:

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending [REDACTED] investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

b6

b7c

e. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

No. The FBI requests only that the provision be preserved.

86. Section 207 of the USA-Patriot Act extends the time limits provided in the FISA which govern surveillance against agents of a foreign power.

a. Has the Federal Bureau of Investigation or the Department of Justice conducted any review to determine whether, and if so, how many, personnel resources have been saved by this provision? If so, please provide the results to the Committee.

Response:

We are not aware of any systematic reviews in this area, either by the FBI or DOJ.

b. Have there been any cases where, after the passage of the now-extended deadlines it was determined, either by the Department of Justice, the Federal Bureau of Investigation or the Foreign Intelligence Surveillance Court, that surveillance should have been terminated at an earlier point because of the absence of a legally required predicate?

Response:

None of which the FBI is aware.

c. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 207 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

b6
b7c

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

None at this time.

87. Section 209 of the USA-Patriot Act clarified the law with regarding the applicability of criminal search warrants to voice mail. This question pertains to application of this provision since its passage.

a. How many such search warrants have been issued since passage of this act?

Response:

The FBI does not collect or maintain statistics concerning the types of search warrants issued in FBI investigations, including those seeking access to voice mail. Because federal search warrants are requested by U.S. Attorneys' Offices and issued by U.S. District Courts, these statistics may be maintained by one or both of those offices.

b. In such cases, have there been any instances in which a wiretap, as opposed to a search[] warrant[,], would not have been supported by the facts asserted in support of the search warrant.

Response:

This information is unavailable, as indicated above. It is clear, however, that the support needed for a federal wiretap is considerably greater than that required for a search warrant.

c. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 209 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

A private citizen who has lodged numerous complaints against the FBI, all of which have been determined to be unfounded pursuant to appropriate inquiry, complained that she was a former FBI employee whose home, vehicles, telephone, and internet had been subject to "aggressive surveillance" since August 2000. FBI investigation revealed that the complainant was, in fact, not a former FBI employee and that the FBI had conducted no surveillance of her for any reason. Based on these findings, this matter was closed by the FBI in July 2003. The FBI has construed this as a complaint with respect to both Section 209 and 217 of the USA PATRIOT Act.

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

The FBI is not aware of any substantive changes to this provision warranting Congressional consideration. Section 209 is, however, currently scheduled to expire at the end of 2005, and the FBI strongly supports making this provision permanent. Section 209 allows investigators to use court-ordered search warrants to obtain voice-mail messages held by a third party provider when supported by probable cause. Previously, the Electronic Communications Privacy Act (ECPA), 18 U.S.C. 2703, allowed law enforcement authorities to use search warrants to gain access to stored electronic communications such as e-mail, but not stored wire communications such as voice-mail. Instead, the wiretap statute, 18 U.S.C. 2110(1), governed access to stored wire communications, requiring law enforcement officers to use wiretap orders to gain access to unopened voice-mail. This resulted in voice-mail messages being treated differently than e-mail messages. Voice-mail messages are also treated differently than answering machine messages inside a home, access to which requires a search warrant, because answering machine messages are not regulated under the wiretap statute. Section 209 of the USA PATRIOT Act eliminates the disparate treatment of similar information. If this section is sunsetted, voice-mail messages will again be treated in a different manner than answering machine messages and stored e-mail information beginning in 2006.

88. Section 212 of the USA-Patriot Act permits communications service providers to provide customer records or the content of customer communications to the FBI in an emergency situation. This question pertains to application of this provision since its passage, and to all instances, not only to terrorism investigations.

a. In how many cases has this provision been used? Please provide a short description of each such case to the Committee.

Response:

Service providers have voluntarily provided information on at least 141 occasions under this provision. Such disclosures have often included both e-mail content and associated records. Several of these disclosures have directly supported terrorism cases under the emergency of a possible pending attack. For example, this provision has been used to obtain access to e-mail accounts used by terrorist groups to discuss various terrorist attacks. It has also been used to respond quickly to bomb and death threats, as well as in an investigation into a threat to a high ranking foreign official. This provision has additionally been used to locate kidnaping victims and to protect children in child exploitation cases. In one kidnaping case involving the abduction of a 14-year-old girl, reliance on this

provision allowed the FBI to quickly locate and rescue the child and to identify and arrest the perpetrator. Because of this provision, additional harm to the girl was prevented and she was returned to her family in a matter of hours.

Because many international service providers are located within the United States (such as [REDACTED]), Legal Attachés have used this provision to assist foreign law enforcement officials with similar emergencies, such as death threats on prosecutors and other foreign officials. Where time is of the essence, giving service providers the option of revealing this information without a court order or grand jury subpoena is crucial to receiving the information quickly and preventing loss of life or serious injury.

b2
b7E

Additional examples are provided in DOJ's July 2004 "Report from the Field: The USA PATRIOT Act at Work."

b. In any such case have there been any cases in which, except for the time constraints imposed by the emergency situation, a conventional wiretap or search warrant, would not have been supported by the facts available to the Government at the time of the emergency request? If so, please describe such situations.

Response:

We are aware of no such circumstances. However, it is important to recognize that the information that may be disclosed under this emergency authority is limited to the contents of communications that are in electronic storage and records associated with customers or subscribers. Given this limitation, a conventional wiretap would generally not apply, and a search warrant would be required only for the contents of communications in 'electronic storage' (e.g., incoming email not yet retrieved by the subscriber) less than 181 days old. Emergency authority is appropriate for the disclosure of information held by a third party and, to the extent the information is constitutionally protected, disclosure of the information under exigent circumstances is entirely consistent with the emergency exception to the warrant requirement of the Fourth Amendment.

c. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 212 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the [REDACTED] [REDACTED] none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

b6

b7c

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

There is currently a discrepancy between the emergency provisions applicable to contents and records that appears illogical and unjustified. Currently a provider is arguably required under 18 U.S.C. 2702(c)(4) to meet a higher burden for disclosing a record or other subscriber information than is required by § 2702(b)(7) for divulging the contents of a communication in electronic storage. Moreover, the entities to whom a provider may disclose are significantly more restricted for records than for content. The language in (b)(7) was enacted by Pub. L. 107-296 as part of the Homeland Security Act of 2002, with the objective that all entities with responsibility for ensuring our domestic security would have access to this information in an emergency. It does not appear that the discrepancies between the disclosure of content and records are supported by differing privacy interests inherent in the respective information or by other factors. Accordingly, reconciling these provisions would be appropriate.

89. Section 214 of the USA-Patriot Act permits the use of FISA pen register/trap & trace orders with respect to electronic communications, and eliminates the requirement that such use be only in the context of a terrorist or espionage investigation. This question pertains to application of this provision since its passage, and to all instances, not only terrorism investigations.

a. In how many cases has this authority been used?

(i) How many of such cases were terrorism-related?

Response to a and a(i):

The FBI does not maintain this information. It is, instead, maintained by DOJ's OIPR, to whom the FBI defers for response.

b. Of the cases in which such authority was used, in how many was a subsequent application for a full surveillance order made pursuant to the FISA, or Chapter 19 of Title 18?

Response:

--

b5

c. Has the Intelligence Community, Department of Justice, or Federal Bureau of Investigation developed regulations or directives defining the meaning of non-content communications? If such regulations or directives have been issued, please provide copies to the Committee.

Response:

The FBI has not developed any such regulations or directives, nor is it aware that the IC or DOJ have issued guidance defining "non-content communications" in relation to the use of FISA pen register/trap and trace authorities.

d. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

Response:

See response to Question 85b, above.

(i) If so, how many such reports have been issued?

Response:

See response to Question 85b(i), above.

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

See response to Question 85b(ii), above.

90. Section 215 of the USA-Patriot [A]ct authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application of this provision since its inception.

a. How many times has this authority been used, and with what success?

Response:

By letter of 12/23/04, the Department provided to the Committee the number of times, if any, authorities under section 1861 of the Foreign Intelligence Surveillance Act (FISA), as amended, had been approved by the Foreign Intelligence Surveillance Court. This semiannual report was submitted pursuant to section 1862(b) of the FISA, and covered the period 1/1/04 through 6/31/04.

b. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.

Response:

The Department provides information pertaining to the operational use of authorities under section 1861 of the FISA to the Senate and House Intelligence Committees on a semiannual basis, pursuant to section 1862(a) of the FISA. The last semiannual report under this section was dated 12/23/04, and covered the period 1/1/04 through 6/31/04. It is our understanding that under applicable Senate Rules and procedures, all Senators are permitted to review this semiannual report upon request to the Senate Select Committee on Intelligence.

c. In your testimony you compared this provision with existing authority in the criminal context, noting that records such as library records are subject to a grand jury subpoena. However, in criminal cases the propriety and lawfulness of subpoenas are to some extent tested in the adversary process of a trial - how, in the context of the FISA, does such a check occur?

Response:

The checks on the use of the business record provision are numerous. First, requests for such orders must be approved by several authorities within the FBI and DOJ to ensure they comply with FISA requirements. In addition, however, business record requests must be approved by a FISA Court judge. FISA judges are part of an independent judiciary, appointed pursuant to Article III of the U.S. Constitution.

Business record orders require a showing that the record is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. "Authorized investigations" may only be initiated when consistent with Attorney General guidelines, so the existence of such an investigation and the relevance of the record to this investigation represent two "checks" on this authority. Under both the Attorney General guidelines and section 215 of the USA PATRIOT Act, such investigations may not be conducted solely on the basis of activities protected by the First Amendment.

Once an appropriate FBI authority determines that a business record order request is relevant to a properly authorized investigation, the request itself requires numerous layers of approval (as do requests for electronic surveillance, physical search, and pen register/trap and trace orders under FISA).

b2
b7E

When presented to the FISA Court, the FISA judge must determine that the request meets FISA requirements before issuing the order.

Lastly, section 215 imposes Congressional oversight by requiring the Attorney General to report to Congress annually on the FBI's use of the section.

d. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

Response:

The only instance when the Department has declassified the number of times section 215 has been used was on 9/18/03 – not in October 2004. At that time (September 2003), Attorney General Ashcroft indicated section 215 had never been used. However, section 215 requires the Department to transmit on a semi-annual basis a report informing Congress of the number of times section 215 has been used. The most recent report was dated 12/23/04.

The PATRIOT Act specifically protects Americans' First Amendment rights, and terrorism investigators have no interest in the library habits of ordinary Americans. Historically, however, terrorists and spies have used libraries to plan and carry out activities that threaten our national security, and it is important that we not permit these facilities to become safe havens for terrorist or other illegal activities. The PATRIOT Act permits those conducting national security investigations to obtain business records – whether from a library or any other business – with the permission of a federal judge.

(i) With respect to the potential applicability of this section to libraries and bookstores, there has been some concern that the mere prospect of use of the statute has a "chilling effect" on the use of these facilities. Can this chilling effect be minimized, if not eliminated, by incorporating a higher threshold for use in the limited context of libraries and bookstores? If not, why not?

Response:

In the context of this question, the FBI can initiate investigations of individuals or groups only under specific conditions articulated in the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG). Additionally, FBI guidelines place strict limits on the types of investigative activities that can be undertaken when investigations are opened, requiring, for example, that no investigation of a U.S. person may be conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

Individuals' rights are additionally safeguarded by other authorities, such as Executive Order (E.O.) 12333, which is the primary authority for intelligence

activities conducted by the IC. E.O. 12333 establishes goals for the collection of intelligence information; assigns responsibilities among the various intelligence components; prescribes what information may be collected, retained, and disseminated; and prescribes or proscribes the use of specified techniques in the collection of intelligence information. As noted above, the NSIG establishes limits and requirements governing FBI international terrorism investigations with respect to foreign intelligence, CI, and intelligence support activities. Another important internal safeguard is the Intelligence Oversight Board (IOB), which reviews the FBI's practices and procedures relating to foreign intelligence and foreign CI, requiring the FBI to report violations of foreign CI or other guidelines designed in full or in part to ensure the protection of the individual rights of a U.S. person.

e. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

Response:

The IIR is the mechanism by which the FBI disseminates raw intelligence information to the Intelligence, Defense, and law enforcement communities. The intelligence information contained in these IIRs is information generally derived from FBI operations, investigations, or sources. Intelligence information acquired pursuant to Section 215 of the USA PATRIOT Act could be disseminated via an IIR in appropriate circumstances. Between August 2002 and August 2004, the FBI has disseminated approximately 3,860 terrorism-related IIRs.

(i) If so, how many such reports have been issued?

Response:

b5

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

Although the FBI has procedures to evaluate the quality of intelligence reports, no reports have been disseminated which contained information acquired pursuant to section 215 of the USA PATRIOT Act.

f. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the pending [REDACTED] investigation, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

b6

b7C

g. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

The FBI has identified no need for change at this time.

91. Section 217 of the USA-Patriot Act authorizes, without court order, the interception of communications to and from a trespasser with a protected computer. This question pertains to the implementation of this provision since its passage.

a. How many times has the authority under this section been used, and with what success? Please provide descriptions of the circumstances where it has been used.

Response:

While the FBI does not maintain statistics on the frequency with which the trespasser authority has been used, we can provide examples of some such cases.

Under this provision, the FBI was able to monitor the communications of an international group of "carders" (individuals who use and trade stolen credit card information). This group used chat rooms and fraudulent web sites, creating false identities to obtain e-mail accounts and then transmitting their communications through a computer that had been "hacked" and set up to operate as their proxy server. A proxy server changes an Internet user's original Internet protocol (IP) address to that of the proxy server so that only the proxy server knows the true point of origin. The owner of the hacked computer was not aware that it was being used as a proxy server, and considered all individuals using the system as a proxy server to be trespassers. The owner provided the FBI with consent to monitor the communication ports solely used by the trespassers, and this monitoring led to the subject's true identity. The subject was indicted in September 2003. Without this authority to monitor, the real identities of the trespassers could easily have remained anonymous.

In another example, a former employee was suspected of illegally accessing a company's e-mail system to gain inside information regarding company concepts and client information, as well as privileged information regarding legal proceedings between the company and the former employee. The computer intruder used a variety of means to access the system, including wireless modems in laptops and hand-held Blackberry devices, making it more difficult to identify the intruder and to link the computer intrusions to the former employee. The victim company authorized the FBI to monitor the intruder's communications with and through its computer systems.

In another case, a computer-intruder obtained control of a school's network and reconfigured it to establish additional IP addresses that were separate and distinct from those used by the school. This allowed hackers, and others using the Internet who did not want to be located, to jump through the school's system before committing their illegal acts. Monitoring accomplished pursuant to the school's consent resulted in the FBI's identification of over 200,000 different IP addresses using the school system as a proxy to further illegal activity such as fraud, computer intrusions, and spamming.

As these cases make clear, this authority is critical not only to the FBI's ability to identify criminals who engage in computer intrusions but also its ability to

identify and investigate additional criminal activities conducted through victims' computers.

b. Section 217(2)(I) requires authorization by the owner of the computer before the section can be applied. Can this authorization be withdrawn or limited by the owner of the computer? If so, how and in what circumstances?

Response:

Yes. As with any form of consent, which must be freely and voluntarily given to be valid, the consenting party has the right to terminate the consent at any time. The FBI encourages the use of a written consent form containing an express acknowledgment by the consenting owner or operator that states: "I understand my right to refuse authorization for interception and have accordingly given this authorization freely and voluntarily."

c. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 217 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

Response:

See response to Question 87c, above.

92. Section 218 of the USA-Patriot Act created the so-called "significant purpose" test for applications pursuant the FISA, clarifying the law to recognize that in many cases such surveillance may implicate both a law enforcement and an intelligence interest. This question pertains to the implementation of this provision since its passage.

a. Please provide the Committee with specific examples, in unclassified form if possible, of cases in which both law enforcement and intelligence interests were "significant."

Response:

As indicated in the July 2004 DOJ publication entitled, "Report from the Field: The USA PATRIOT Act at Work," the removal of the "wall" played a crucial role in the Department's successful dismantling of a Portland, Oregon, terror cell, popularly known as the "Portland Seven." Members of this terror cell had

attempted to travel to Afghanistan in 2001 and 2002 to take up arms with the Taliban and al Qaeda against United States and coalition forces fighting there. Law enforcement agents investigating that case learned through an undercover informant that [REDACTED]

[REDACTED] While several of these other individuals had returned to the United States from their unsuccessful attempts to reach Afghanistan, investigators did not yet have sufficient evidence to arrest them. Before the USA PATRIOT Act, prosecutors would have faced a dilemma in deciding whether to arrest [REDACTED] immediately. If prosecutors had failed to act, lives could have been lost through a domestic terrorist attack; if prosecutors had arrested [REDACTED] in order to prevent a potential attack, the other suspects in the investigation would undoubtedly have scattered or attempted to cover up their crimes. Because of sections 218 and 504 of the USA PATRIOT Act, however, FBI agents could conduct FISA surveillance of [REDACTED] to detect whether he had received orders from an international terrorist group to reinstate the domestic attack plan on Jewish targets, and could keep prosecutors informed as to what they were learning. This gave prosecutors the confidence not to arrest [REDACTED] prematurely, but instead to continue to gather evidence on the other cell members. Ultimately, prosecutors were able to collect sufficient evidence to charge seven defendants and then to secure convictions and prison sentences ranging from three to eighteen years for the six defendants taken into custody. Charges against the seventh defendant were dismissed after he was killed in Pakistan by Pakistani troops on 10/3/03.

b6
b7C
b7D

DOJ shared information pursuant to sections 218 and 504 before indicting [REDACTED] and several co-conspirators on charges related to their involvement with the Palestinian Islamic Jihad (PIJ). PIJ is alleged to be one of the world's most violent terrorist organizations, responsible for murdering over 100 innocent people, including Alisa Flatow, a young American killed in a bus bombing near the Israeli settlement of Kfar Darom. The indictment states that [REDACTED] served as the secretary of the PIJ's governing council ("Shura Council"). He was also identified as the senior North American representative of the PIJ. Sections 218 and 504 of the USA PATRIOT Act enabled prosecutors to consider all evidence against [REDACTED] and his co-conspirators, including evidence obtained pursuant to FISA that provided the necessary factual support for the criminal case. By considering the intelligence and law enforcement information together, prosecutors were able to create a complete history for the case and put each piece of evidence in its proper context. This comprehensive approach was essential to prosecutors' ability to build their case and pursue the proper charges.

b6
b7C

Prosecutors and investigators also used information shared pursuant to sections 218 and 504 of the USA PATRIOT Act in investigating the defendants in the so-called "Virginia Jihad" case. This prosecution involved members of the Dar al-Arqam Islamic Center, some of whom trained for jihad in Northern Virginia by participating in paintball and paramilitary training or traveled to terrorist training camps in Pakistan or Afghanistan between 1999 and 2001. These individuals are associates of a violent Islamic extremist group known as Lashkar-e-Taiba (LET), which primarily operates in Pakistan and Kashmir and has ties to the al Qaeda terrorist network. As the result of an investigation that included the use of information obtained through FISA, prosecutors were able to bring charges against several individuals. Nine of these defendants have received sentences ranging from four years to life imprisonment (six of these sentences were pursuant to guilty pleas and three were contrary to their pleas; charges have included conspiracy to levy war against the United States and conspiracy to provide material support to the Taliban).

Information sharing between intelligence and law enforcement personnel made possible by sections 218 and 504 of the USA PATRIOT Act was also pivotal in the investigation of two Yemeni citizens [redacted] and [redacted] who were charged in 2003 with conspiring to provide material support to al Qaeda and HAMAS. [redacted]

[redacted] the complaint alleges that [redacted] had boasted that he had personally handed Usama Bin Laden \$20 million from his terrorist fund-raising network and that [redacted] had flown from Yemen to Frankfurt, Germany, in 2003 with the intent to obtain \$2 million from a terrorist sympathizer [redacted] who wanted to fund al Qaeda and HAMAS. During their meetings, [redacted]

b6
b7C
b7D

[redacted]
[redacted] were extradited to the United States from Germany in November 2003 and are currently awaiting trial.

Sections 218 and 504 were also used to gain access to intelligence that facilitated the indictment of [redacted] Benevolence International Foundation (BIF). [redacted] conspired to fraudulently obtain charitable donations in order to provide financial assistance to Chechen rebels and organizations engaged in violence and terrorism. [redacted] had a long-standing relationship with Usama Bin Laden, and used his charities both to obtain funds for terrorist organizations from unsuspecting Americans and to serve as a channel for people to contribute money knowingly to such groups. [redacted] pled guilty to a racketeering charge, admitting that he diverted thousands of dollars from BIF to support Islamic militant groups in Bosnia and Chechnya. He was sentenced to over 11 years in prison.

b6
b7C

The broader information sharing and coordination made possible by sections 218 and 504 of the USA PATRIOT Act assisted the San Diego prosecution of several persons involved in an al Qaeda drugs-for-weapons plot, which culminated in several guilty pleas. Two defendants admitted that they had conspired to distribute approximately five metric tons of hashish and 600 kilograms of heroin originating in Pakistan to undercover United States law enforcement officers. Additionally, they admitted that they had conspired to receive, as partial payment for the drugs, four "Stinger" anti-aircraft missiles that they then intended to sell to the Taliban, an organization they knew at the time to be affiliated with al Qaeda. The lead defendant in the case is currently awaiting trial.

Sections 218 and 504 were also critical in the successful prosecution of [redacted] who was convicted by a jury in January 2004 of illegally acting as an agent of the former government of Iraq and of two counts of perjury. Before the Gulf War [redacted] passed information on Iraqi opposition members located in the United States to officers of the Iraqi Intelligence Service stationed in the Iraqi Mission to the United Nations. During this investigation, intelligence officers conducting surveillance of [redacted] pursuant to FISA shared information with law enforcement agents and prosecutors investigating [redacted]. Through this coordination, law enforcement agents and prosecutors learned from intelligence officers that [redacted] [redacted] was acting as an agent of the Iraqi government, providing a compelling piece of evidence at [redacted] trial.

b6
b7C

b. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 218 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

Response:

The Department's Office of the Inspector General (OIG) is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

b6
b7C

The OIG has advised that, with the possible exception of the [redacted] [redacted] none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA

PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

c. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

The FISA Court of Review has made clear that the "significant purpose" standard is constitutional. Accordingly, additional changes are unnecessary.

93. Section 220 of the USA-Patriot Act, "Nationwide Service of Search Warrants for Electronic Evidence" allows for the execution of a search warrant seeking electronic data anywhere in the country. This question pertains to the implementation of this provision since its passage.

a. In how many cases has this authority been used?

Response:

While the FBI does not require or maintain centralized statistics on the use of search warrants, Field Offices indicate that they have routinely relied on this provision (codified at 18 U.S.C. 2703(a)) and can safely estimate that, nationwide, this search authority has been used at least 100 times since its passage.

In section 220 of the USA PATRIOT Act, Congress adapted federal law to changing technology by allowing courts to order the release of stored communications through a search warrant valid in another specified judicial district. The ability to obtain this information with greater efficiency has proven invaluable in numerous cases, including: several terrorism investigations (such as the Virginia Jihad case described above and a complex terrorism financing case in which it was used to obtain a subject's e-mail related to a 7/4/02 shooting at Los Angeles International Airport); child pornography cases in which it is used to obtain information from ISPs regarding those trading sexually exploitive images of children; investigations of "carders" (those who use and trade stolen credit card information); and numerous investigations into Internet sales of counterfeit products, which have led to several indictments and the seizure of bank and financial accounts.

Child pornography cases highlight the benefit of Section 220, because the ability to obtain a search warrant in the jurisdiction of a child pornography investigation rather than in the jurisdiction of the ISP is critical to the success of a complex, multi-jurisdictional child pornography case. In the absence of section 220, law enforcement agents would either have to spend hours briefing other agents across the country so they could obtain warrants in those jurisdictions, or travel hundreds or thousands of miles to present warrant applications to local magistrate judges. Without Section 220, one of two things would often occur in light of limited law enforcement resources: either the scope of the investigation would be narrowed or the case would be deemed impractical at the outset and dropped.

The following case, included in DOJ's July 2004 "Report from the Field: The USA PATRIOT Act at Work," provides an additional example of the benefits afforded by Section 220. A man, armed with a sawed-off shotgun, abducted his estranged wife and sexually assaulted her. Then, after releasing his wife, he fled West Virginia in a stolen car to avoid capture. While in flight, he contacted cooperating individuals by e-mail using an Internet service provider (ISP) located in California. Using the authority provided by section 220, investigators in West Virginia were able to obtain an order from a federal court in West Virginia for the disclosure of information regarding the armed fugitive's e-mail account, including the California ISP. Within a day of the order's issuance, the ISP released information revealing that the fugitive had contacted individuals from a public library in a small town in South Carolina. The very next day, Deputy U.S. Marshals went to the town and noticed a carnival set up next to the public library. Because they were aware that the fugitive had previously worked as a carnival worker, the Deputy Marshals went to the carnival and discovered the stolen car, arresting the fugitive as he approached the car. He later pled guilty in state court and was sentenced to imprisonment for 30 years. In this case, the fast turn-around on the order for information related to the fugitive's e-mail account, made possible by section 220 of the USA PATRIOT Act, was crucial to his capture.

Section 220 has also made the process of obtaining a warrant for ISP information much more efficient. Before the USA PATRIOT Act, judicial districts that are home to large ISPs were inundated with search warrant requests for electronic evidence. For example, the U.S. Attorney's Office in Alexandria, Virginia, was receiving approximately 10 applications each month from United States Attorney's Offices in other districts for search warrants for the records of an ISP located there. For each of these applications, an Assistant United States Attorney in Virginia and a law enforcement agent in the district had to learn all the details of another district's investigation in order to present an affidavit to the court in support of the search warrant application. Because of section 220, however, these attorneys and Agents can now spend their time on local cases and investigations rather than on learning the details of unrelated investigations being worked

through distant offices. Given the short time for which ISPs typically retain records, this provision has enabled the FBI to obtain critical information that may otherwise have been lost or destroyed in the ordinary course of the ISP's business. Section 220 also results in a more efficient use of judicial resources by allowing the judge with jurisdiction over the offense to issue the warrant and retain oversight over the search.

b. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 220 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

Response:

The DOJ OIG is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by DOJ employees. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of the [REDACTED] [REDACTED] none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

b6
b7c

c. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

No. The FBI requests only that the provision be preserved.

94. Section 223 of the USA-Patriot Act creates a cause of action for willful violations of Title III's electronic surveillance procedures. Have any such lawsuits been brought? If so, please provide details of each such case.

Response:

No such lawsuits have been brought.

95. Section 225 of the USA-Patriot Act provides immunity for those who aid in the execution of a FISA order. Has such immunity been invoked? If so, please describe any such case.

Response:

No. Immunity has not been claimed under this section with respect to FBI investigations in either the civil or criminal context.

96. The following question pertains to surveillance conducted pursuant to the FISA.

a. What is the backlog on processing of intercepts? What is the average time between interception and first monitoring.

b. What percentage of intercepts that are not in English are translated within 24 hours? A week?

c. How many hours of FISA intercepts remain untranslated as of May 20, 2004?

Response to a through c:

FBI Director Mueller has made clear his interest in having all material derived from the FBI's use of FISA authority reviewed and analyzed as quickly as possible. Since the majority of this material is in languages other than English, FBI Language Services Section personnel meet with the FBI's National FISA Manager and other management officials every two weeks to discuss national operational priorities and the most effective utilization of finite linguist resources. The operational plan established by this meeting is modified almost daily based on ever-shifting investigative priorities. These tactics ensure that all of the highest priority intelligence collected in a foreign language is reviewed immediately and that any outstanding work is limited to matters assigned a lower relative priority.

The FBI currently has sufficient translation capacity to promptly address all translation needs with respect to its highest priority, CT operations, often within 12 hours. While there are instances in which the FBI is not able to address translation needs as quickly as it would like, such as when the language or dialect involved is initially unidentifiable, this usually pertains to lower priority matters.

Conventional digital systems used to collect FISA-derived materials were not designed to measure the average time between intercept and initial monitoring. Recognizing the tactical value of having such aging reports for command and control purposes, a nationally integrated FISA statistical collection and reporting system has been developed and is undergoing a test and evaluation process to validate the mapping of meta data. This system should be fully functional by the end of calendar year 2004. It is clear, however, based on information provided by FBI field office managers, that the vast majority of communications in a foreign language relating to terrorism operations are being afforded full review by a qualified linguist within, at most, a few days of collection.

d. Please describe the process of indexing and retrieving FISA material.

Response:

Intelligence summaries from FISA intercepts are indexed and archived according to strict electronic surveillance (ELSUR) rules that make these summaries part of the official FBI record and allow these records to be searched in the Field Offices where the cases reside. Although recent progress has been made in creating an electronic archive of CI material that can be searched by authorized users fieldwide, CT summaries from FISA audio intercepts are not searchable in a central database at this time. The phased deployment of the ELSUR Data Management System (EDMS), starting in FY 2005, will make all intelligence summaries from FISA intercepts available in a searchable archive.

e. In the past 5 years, has there been a review or audit of the accuracy of FBI translations of intercepted or seized foreign language material?

Response:

Historically, translation reviews were normally conducted by field office managers on a semi-annual basis in conjunction with a linguist's performance appraisal rating. In order to standardize this procedure, the FBI's Language Services Section implemented minimum quality control standards and guidelines and assumed central management of the language services quality control program in January 2003. Quality control program guidelines stipulate which linguists' translations must be reviewed and at what intervals. The guidelines also identify those materials that must always be reviewed prior to dissemination.

Questions Posed by Senator Feingold

FBI Role in Iraq

97. a. How many special agents, translators, and other FBI employees have been assigned to work in Iraq since March 2003 and how many are currently there?

Response:

The response to this question is classified and is, therefore, provided separately.

b. Where were these agents, translators, and other employees assigned before they were sent to Iraq?

Response:

They were assigned to many of the FBI's offices, both in the field and at FBIHQ.

c. How many of these agents, translators, and other employees were working in the United States on terrorism cases?

Response:

15 percent of the FBI employees sent to Iraq were working on terrorism cases prior to that deployment.

FBI DNA Lab

98. The U.S. Department of Justice and Jacqueline Blake, a former biologist at the FBI DNA laboratory, recently entered into a plea agreement. Blake pled guilty to authoring and submitting over 100 reports containing false statements regarding DNA analysis she performed during a 2-1/2 year period from 1999 to 2002.

a. According to a Justice Department press release, the FBI has retested evidence in many of Blake's cases and has concluded that her false statements did not affect the outcome of any of the criminal cases in which she was involved. I assume that the FBI has notified the prosecutors in those cases. Has the FBI notified the courts and defense attorneys in each case in which Blake's falsified reports were involved? If not, why not?

sufficient to justify the delay. In addition, notice is only delayed; it is never eliminated. The searched party will, therefore, have the opportunity to challenge the validity and sufficiency of the reasons for delay and, if those reasons prove to be insufficient, to seek an appropriate remedy.

d. How many of the delayed notice warrants were issued with a (i) seven-day or less delay; (ii) 8 to 30 day delay; (iii) 31 to 60 day delay; and (iv) time period of 61 days or more and what were those time periods?

e. How many of the delayed notification warrants issued since the PATRIOT Act was passed were used in non-terrorism criminal matters?

f. Please provide the case name, docket number, and court of jurisdiction for each case in which a delayed notice warrant was issued since enactment of the PATRIOT Act.

Response to d through f:

This information was not collected in the EOUSA survey and is not otherwise available except through individual U.S. Attorney's Offices.

103. In September 2003, the U.S. Department of Justice disclosed that it had not yet used section 215 of the USA PATRIOT Act. On March 9, 2004, I sent a letter to the Attorney General asking him to clarify whether section 215 has been used since September 18, 2003. (Copy of letter attached.)

a. Please indicate whether section 215 has been used since September 18, 2003.

Response:

By letter of 12/23/04, the Department provided to the Committee the number of times, if any, authorities under section 1861 of the Foreign Intelligence Surveillance Act (FISA), as amended, had been approved by the Foreign Intelligence Surveillance Court. This semiannual report was submitted pursuant to section 1862(b) of the FISA, and covered the period 1/1/04 through 6/31/04.

b. If section 215 has been used, please describe how it has been used. How many U.S. persons and non-U.S. persons were targets of the investigation? Was the section 215 order served on a library, newsroom, or other First Amendment sensitive place? Was the product of the search used in a criminal prosecution?

Response:

The Department provides information pertaining to the operational use of authorities under section 1861 of the FISA to the Senate and House Intelligence Committees on a semiannual basis, pursuant to section 1862(a) of the FISA. The last semiannual report under this section was dated 12/23/04, and covered the period 1/1/04 through 6/31/04. It is our understanding that under applicable Senate Rules and procedures, all Senators are permitted to review this semiannual report upon request to the Senate Select Committee on Intelligence.

104. The Security and Freedom Ensured (SAFE) Act (S. 1709) would amend the roving wiretaps provision of the PATRIOT Act (section 206) by placing reasonable safeguards to protect the conversations of innocent Americans.

a. The SAFE Act would require the FBI to determine whether the target of the wiretap is present at the place being tapped. Since the FBI must already comply with this requirement when conducting roving wiretaps in criminal investigations (*see* 18 U.S.C. § 2518(11), (12)), why shouldn't Congress require the FBI to comply with this important requirement when conducting roving wiretaps in foreign intelligence investigations? Please explain.

Response:

The requirements of the SAFE Act are inconsistent with, and more restrictive than, the requirements applicable to roving wiretaps in criminal investigations. In criminal cases, roving wiretap orders are limited to "such time as it is reasonable to presume that the [target] is or was reasonably proximate" to the facility. 18 U.S.C. 2518(11)(b)(iv). This does not require a conclusive determination that the target is actually present at the time of interception, as the SAFE Act would require, but only a reasonable belief under the circumstances that the facility or place is being used by the target. An analogous requirement is already contained in the Foreign Intelligence Surveillance Act (FISA). Under FISA, the FBI must demonstrate probable cause to believe that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. 1805(a)(3)(B). In addition to these safeguards, both Title III and FISA require the use of procedures

90. Section 215 of the USA-Patriot [A]ct authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application of this provision since its inception.

a. How many times has this authority been used, and with what success?

Response:

By letter of December 23, 2004, the Department provided to the Committee the number of times, if any, authorities under section 1861 of the Foreign Intelligence Surveillance Act (FISA), as amended, had been approved by the Foreign Intelligence Surveillance Court. This semiannual report was submitted pursuant to section 1862(b) of the FISA, and covered the period January 1, 2004 through June 31, 2004.

b. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.

Response:

The Department provides information pertaining to the operational use of authorities under section 1861 of the FISA to the Senate and House Intelligence Committees on a semiannual basis, pursuant to section 1862(a) of the FISA. The last semiannual report under this section was dated December 23, 2004, and covered the period January 1, 2004 through June 31, 2004. It is our understanding that under applicable Senate Rules and procedures, all Senators are permitted to review this semiannual report upon request to the Senate Select Committee on Intelligence.

c. In your testimony you compared this provision with existing authority in the criminal context, noting that records such as library records are subject to a grand jury subpoena. However, in criminal cases the propriety and lawfulness of subpoenas are to some extent tested in the adversary process of a trial - how, in the context of the FISA, does such a check occur?

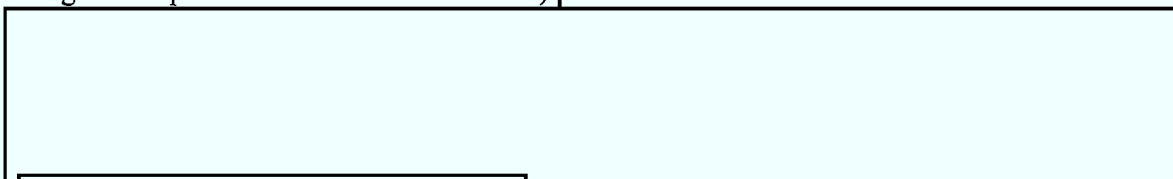
Response:

The checks on the use of the business record provision are numerous. First, requests for such orders must be approved by several authorities within the FBI and DOJ to ensure they comply with FISA requirements. In addition, however, business record requests must be approved by a FISA Court judge. FISA judges are part of an independent judiciary, appointed pursuant to Article III of the U.S. Constitution.

Business record orders require a showing that the record is relevant to an authorized

investigation to protect against international terrorism or clandestine intelligence activities. "Authorized investigations" may only be initiated when consistent with Attorney General guidelines, so the existence of such an investigation and the relevance of the record to this investigation represent two "checks" on this authority. Under both the Attorney General guidelines and section 215 of the USA PATRIOT Act, such investigations may not be premised solely upon the exercise of First Amendment-protected activities.

Once an appropriate FBI authority determines that a business record order request is relevant to a properly authorized investigation, the request itself requires numerous layers of approval (as do requests for electronic surveillance, physical search, and pen register/trap and trace orders under FISA).



b2
b7E

When presented to the FISA Court, the FISA judge must determine that the request meets FISA requirements before issuing the order.

Lastly, section 215 imposes Congressional oversight by requiring the Attorney General to report to Congress annually on the FBI's use of the section.

d. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

Response:

The only instance when the Department has declassified the number of times section 215 has been used was on September 18, 2003 – not October 2004. At that time (September 2003), Attorney General Ashcroft indicated section 215 had never been used. However, section 215 requires the Department to transmit on a semi-annual basis a report informing Congress of the number of times section 215 has been used. The most recent report was dated December 23, 2004.

The PATRIOT Act specifically protects Americans' First Amendment rights, and terrorism investigators have no interest in the library habits of ordinary Americans. Historically, terrorists and spies have used libraries to plan and carry out activities that threaten our national security. If terrorists or spies use libraries, we should not allow them to become safe havens for their terrorist or clandestine activities. The PATRIOT Act ensures that business records – whether from a library or any other business – can be obtained in national security investigations with the permission of a federal judge.

(i) With respect to the potential applicability of this section to libraries and bookstores, there has been some concern that the mere prospect of use of the statute has a "chilling effect" on the use of these facilities. Can this chilling effect be minimized, if not eliminated, by incorporating a higher threshold for use in the limited context of libraries and bookstores? If not, why not?

Response:

In the context of this question, the FBI can initiate investigations of individuals or groups only under specific conditions articulated in the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG). Additionally, FBI guidelines place strict limits on the types of investigative activities that can be undertaken when investigations are opened, requiring, for example, that no investigation of a U.S. person may be conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

Individuals' rights are additionally safeguarded by other authorities, such as Executive Order (E.O.) 12333, which is the primary authority for intelligence activities conducted by the USIC. E.O. 12333 establishes goals for the collection of intelligence information; assigns responsibilities among the various intelligence components; prescribes what information may be collected, retained, and disseminated; and prescribes or proscribes the use of specified techniques in the collection of intelligence information. As noted above, the NSIG establishes limits and requirements governing FBI international terrorism investigations with respect to foreign intelligence, CI, and intelligence support activities. Another important internal safeguard is the Intelligence Oversight Board (IOB), which reviews the FBI's practices and procedures relating to foreign intelligence and foreign CI, requiring the FBI to report violations of foreign CI or other guidelines designed in full or in part to ensure the protection of the individual rights of a U.S. person.

e. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

Response:

The IIR is the mechanism by which the FBI disseminates raw intelligence information to the Intelligence, Defense, and law enforcement communities. The intelligence information contained in these IIRs is information generally derived from FBI operations, investigations, or sources. Intelligence information acquired pursuant to Section 215 of the USA PATRIOT Act could be disseminated via an IIR in appropriate circumstances. Between August 2002 and August 2004, the FBI has disseminated approximately 3,860 terrorism-related IIRs.

(i) If so, how many such reports have been issued?

Response:

b5

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

f. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

The Department's Office of the Inspector General (OIG) is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by employees of the Department of Justice. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of one matter, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

g. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

The FBI has identified no need for change at this time.

90. Section 215 of the USA-Patriot [A]ct authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application of this provision since its inception.

a. How many times has this authority been used, and with what success?

b. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.

Response to a and b:

The responses to these questions are classified and are, therefore, provided separately.

c. In your testimony you compared this provision with existing authority in the criminal context, noting that records such as library records are subject to a grand jury subpoena. However, in criminal cases the propriety and lawfulness of subpoenas are to some extent tested in the adversary process of a trial - how, in the context of the FISA, does such a check occur?

Response:

The checks on the use of the business record provision are numerous. First, requests for such orders must be approved by several authorities within the FBI and DOJ to ensure they comply with FISA requirements. In addition, however, business record requests must be approved by a FISA Court judge. FISA judges are part of an independent judiciary, appointed pursuant to Article III of the U.S. Constitution.

Business record orders require a showing that the record is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. "Authorized investigations" may only be initiated when consistent with Attorney General guidelines, so the existence of such an investigation and the relevance of the record to this investigation represent two "checks" on this authority. Under both the Attorney General guidelines and section 215 of the USA PATRIOT Act, such investigations may not be premised solely upon the exercise of constitutionally protected activities.

Once an appropriate FBI authority determines that a business record order request is relevant to a properly authorized investigation, the request itself requires numerous layers of approval (as do requests for electronic surveillance, physical search, and pen register/trap and trace orders under FISA).

[REDACTED]

b2
b7E

b2

b7E

[REDACTED]

[REDACTED] When presented to the FISA Court, the FISA judge must determine that the request meets FISA requirements before issuing the order.

Lastly, section 215 imposes Congressional oversight by requiring the Attorney General to report to Congress annually on the FBI's use of the section.

d. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

Response:

The response to this question is classified and is, therefore, provided separately.

(i) With respect to the potential applicability of this section to libraries and bookstores, there has been some concern that the mere prospect of use of the statute has a "chilling effect" on the use of these facilities. Can this chilling effect be minimized, if not eliminated, by incorporating a higher threshold for use in the limited context of libraries and bookstores? If not, why not?

Response:

In the context of this question, the FBI can initiate investigations of individuals or groups only under specific conditions articulated in the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG). Additionally, FBI guidelines place strict limits on the types of investigative activities that can be undertaken when investigations are opened, requiring, for example, that no investigation of a U.S. person may be conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

Individuals' rights are additionally safeguarded by other authorities, such as Executive Order (E.O.) 12333, which is the primary authority for intelligence activities conducted by the USIC. E.O. 12333 establishes goals for the collection of intelligence information; assigns responsibilities among the various intelligence components; prescribes what information may be collected, retained, and disseminated; and prescribes or proscribes the use of specified techniques in the collection of intelligence information. As noted above, the NSIG establishes limits and requirements governing FBI international terrorism investigations with respect to foreign intelligence, CI, and intelligence support activities. Another important internal safeguard is the Intelligence Oversight Board (IOB), which reviews the FBI's practices and procedures relating to foreign intelligence and foreign CI, requiring the FBI to report violations of foreign CI or other guidelines designed in full or

in part to ensure the protection of the individual rights of a U.S. person.

e. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

Response:

The IIR is the mechanism by which the FBI disseminates raw intelligence information to the Intelligence, Defense, and law enforcement communities. The intelligence information contained in these IIRs is information generally derived from FBI operations, investigations, or sources. Intelligence information acquired pursuant to Section 215 of the USA PATRIOT Act could be disseminated via an IIR in appropriate circumstances. Between August 2002 and August 2004, the FBI has disseminated approximately 3,860 terrorism-related IIRs.

(i) If so, how many such reports have been issued?

Response:

b5

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response:

f. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

The FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

g. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

The FBI has identified no need for change at this time.

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

90. Section 215 of the USA-Patriot [A]ct authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application of this provision since its inception.

a. How many times has this authority been used, and with what success?

Response:

FBI

(S)

DOJ

By letter of December 23, 2004, the Department provided to the Committee the number of times, if any, authorities under section 1861 of the Foreign Intelligence Surveillance Act (FISA), as amended, had been approved by the Foreign Intelligence Surveillance Court. This semiannual report was submitted pursuant to section 1862(b) of the FISA, and covered the period January 1, 2004 through June 31, 2004.

b1

b2

b7E

b. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.

Response:

FBI

b1

(S)

DOJ

The Department provides information pertaining to the operational use of authorities under section 1861 of the FISA to the Senate and House Intelligence Committees on a semiannual basis, pursuant to section 1862(a) of the FISA. The last semiannual report under this section was dated December 23, 2004, and covered the period January 1, 2004 through June 31, 2004. It is our understanding that under applicable Senate Rules and procedures, all Senators are permitted to review this semiannual report upon request to the Senate Select Committee on Intelligence.

d. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

Response:

FBI

b1

(S)

(S)

~~SECRET~~

~~SECRET~~

(S)

b1
b2
b7E

(S)

DOJ

The only instance when the Department has declassified the number of times section 215 has been used was on September 18, 2003 – not October 2004. At that time (September 2003), Attorney General Ashcroft indicated section 215 had never been used. However, section 215 requires the Department to transmit on a semi-annual basis a report informing Congress of the number of times section 215 has been used. The most recent report was dated December 23, 2004.

The PATRIOT Act specifically protects Americans' First Amendment rights, and terrorism investigators have no interest in the library habits of ordinary Americans. Historically, terrorists and spies have used libraries to plan and carry out activities that threaten our national security. If terrorists or spies use libraries, we should not allow them to become safe havens for their terrorist or clandestine activities. The PATRIOT Act ensures that business records – whether from a library or any other business – can be obtained in national security investigations with the permission of a federal judge.

f. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

FBI

The FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

~~SECRET~~

~~SECRET~~

DOJ

The Department's Office of the Inspector General (OIG) is required under section 1001 of the USA PATRIOT Act to report to Congress every six months on allegations received by the OIG alleging abuses of civil rights or civil liberties by employees of the Department of Justice. The OIG issued its fifth report under section 1001 in September 2004.

The OIG has advised that, with the possible exception of one matter, none of the complaints submitted to the OIG alleging misconduct by employees of the Department has related to the use of a provision of the USA PATRIOT Act. Additionally, the FBI's Inspection Division, which reviews allegations of FBI misconduct, is aware of no complaints with respect to the FBI's application or implementation of this section.

~~SECRET~~

MessageFrom: FOGLE, TONI M. (INSD) (FBI)
Sent: Tuesday, September 14, 2004 2:55 PM
To: [REDACTED] (OCA) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

b6
b7C

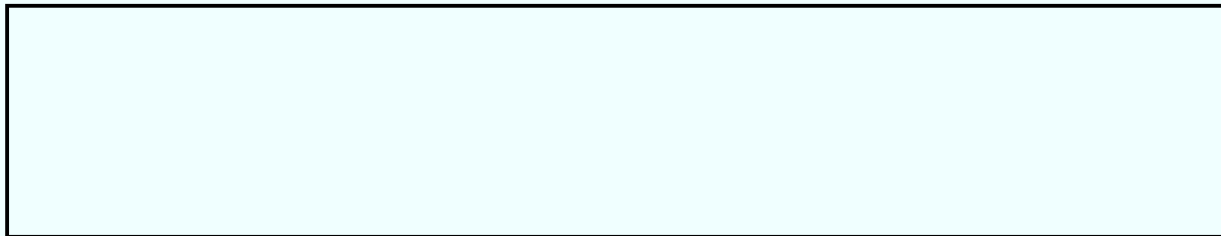
call it a day

-----Original Message-----

From: [REDACTED] (OCA) (FBI)
Sent: Tuesday, September 14, 2004 2:43 PM
To: FOGLE, TONI M. (INSD) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

b5



[REDACTED] b2
Office of Congressional Affairs b6
JEH Building Room 7252 b7C
[REDACTED]

-----Original Message-----

From: FOGLE, TONI M. (INSD) (FBI)
Sent: Tuesday, September 14, 2004 2:41 PM
To: [REDACTED] (OCA) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

b5

-----Original Message-----

From: [REDACTED] OCA) (FBI)
Sent: Tuesday, September 14, 2004 2:11 PM
To: FOGLE, TONI M. (INSD) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED b6
NON-RECORD b7C

Toni:

b5

[REDACTED]
Office of Congressional Affairs
IEH Building Room 7252

b6

b7C

-----Original Message-----

b2

From: FOGLE, TONI M. (INSD) (FBI)
Sent: Tuesday, September 14, 2004 1:43 PM
To: [REDACTED] OCA) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED

NON-RECORD



-----Original Message-----

From: [redacted] (OCA) (FBI)
Sent: Tuesday, September 14, 2004 12:30 PM b6
To: FOGLE, TONI M. (INSD) (FBI) b7C
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD



b5

[redacted]
Office of Congressional Affairs
JEH Building Room 7252

b6

b7C

-----Original Message-----

b2

From: FOGLE, TONI M. (INSD) (FBI)
Sent: Tuesday, September 14, 2004 11:58 AM
To: [redacted] (OCA) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD



b5

-----Original Message-----

From: [redacted] OCA) (FBI)
Sent: Friday, September 10, 2004 4:07 PM
To: FOGLE, TONI M. (INSD) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

b6

b7C

UNCLASSIFIED
NON-RECORD



b5

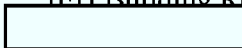


Office of Congressional Affairs
IEH Building Room 7252

b2

b6

b7C



-----Original Message-----

From: FOGLE, TONI M. (INSD) (FBI)
Sent: Friday, September 10, 2004 3:55 PM
To: [redacted] OCA) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

b6
b7C
b5

-----Original Message-----

From: [REDACTED] (OCA) (FBI) b6
Sent: Friday, September 10, 2004 8:21 AM b7C
To: FOGLE, TONI M. (INSD) (FBI)
Subject: FW: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

b6
b7C
b5

Thanks!

[REDACTED]
Office of Congressional Affairs
JEH Building Room 7252

-----Original Message-----

From: THOMPSON, DONALD W. JR (RH) (FBI) b6
Sent: Thursday, September 09, 2004 6:26 PM b7C
To: [REDACTED] (OCA) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

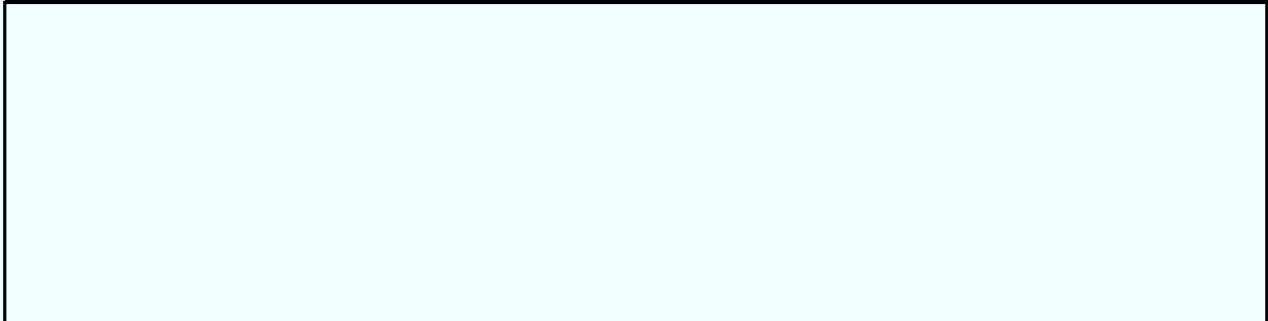
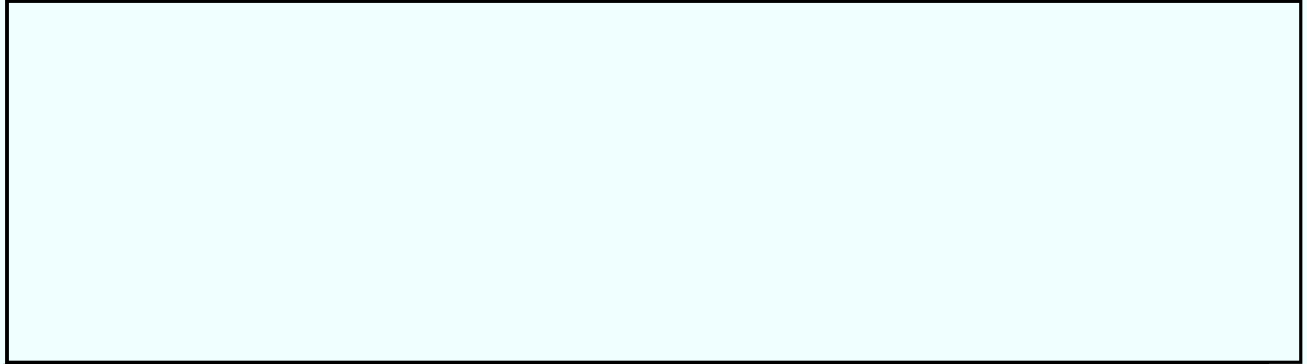
UNCLASSIFIED
NON-RECORD

[REDACTED] I concur with the below responses. Thanks. DWT

-----Original Message-----

From: [REDACTED] (OCA) (FBI)
Sent: Thursday, September 09, 2004 5:54 PM
To: THOMPSON, DONALD W. JR (RH) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD



b5

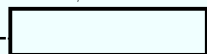
b6

b7C

b5



Thanks.



b2

Office of Congressional Affairs
JEH Building Room 7252

b6

b7C



-----Original Message-----

From: THOMPSON, DONALD W. JR (RH) (FBI)

Sent: Thursday, September 09, 2004 5:42 PM

To: [redacted] (OCA) (FBI)

Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

[Redacted]

b5

-----Original Message-----

From: [Redacted] (OCA) (FBI)

b6

Sent: Thursday, September 09, 2004 2:13 PM

b7C

To: FOGLE, TONLM. (INSD) (FBI)

Cc: [Redacted] (INSD) (FBI); THOMPSON, DONALD W. JR (RH)

(FBI)

Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED

NON-RECORD

b5

A/AD Thompson:

[Redacted]

Thanks.

[Redacted]

Office of Congressional Affairs
JEH Building Room 7252

[Redacted]

-----Original Message-----

From: FOGLE, TONI M. (INSD) (FBI)

Sent: Thursday, September 09, 2004 2:11 PM

b2

To: [Redacted] (OCA) (FBI)

b6

Cc: [Redacted] (INSD) (FBI); THOMPSON, DONALD W. JR (RH)

b7C

(FBI)

Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED

NON-RECORD

[Redacted]

Could you work out the language with A/AD Thompson this afternoon (I'm in a meeting that may take some time) -- leaving open this one situation? I'll ask [Redacted] to work on the

questions you've asked on this open situation. T>

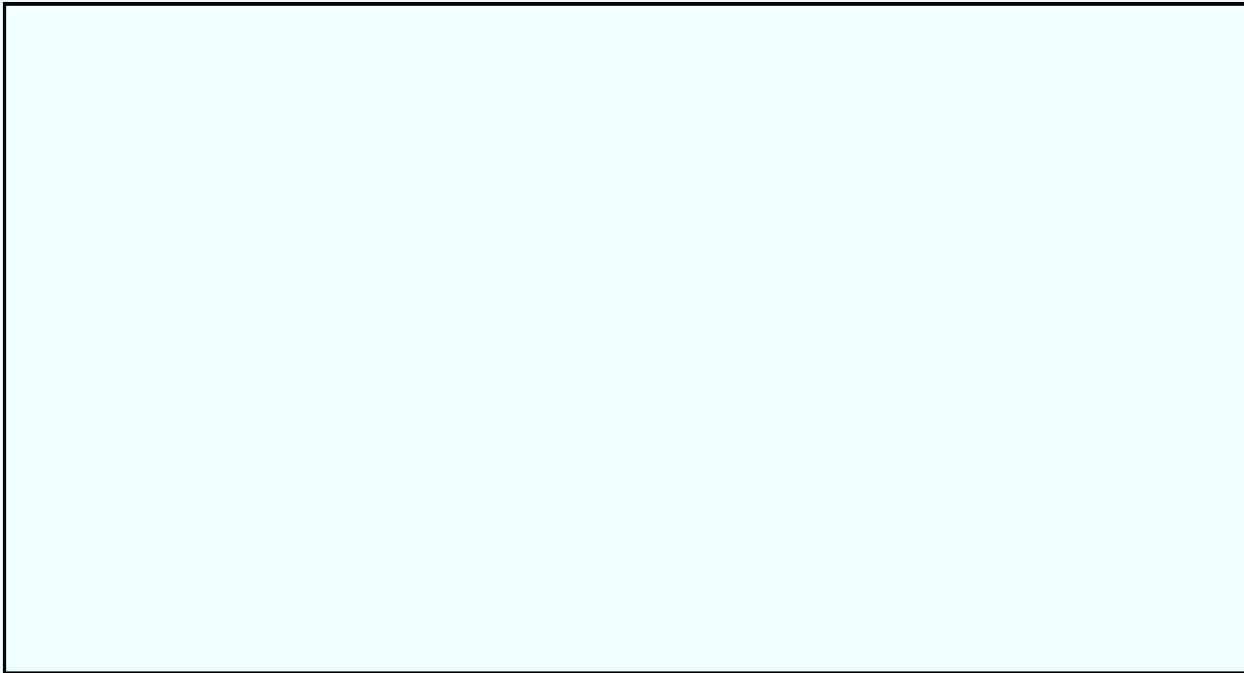
-----Original Message-----

From: [REDACTED] (OCA) (FBI)
Sent: Thursday, September 09, 2004 2:04 PM
To: FOGLE, TONI M. (INSD) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

b6

b7C

UNCLASSIFIED
NON-RECORD



b6

b7C

b5

[REDACTED]
Office of Congressional Affairs
JEH Building Room 7252

b2

b6

-----Original Message-----

b7C

From: [REDACTED] (INSD) (FBI)
Sent: Thursday, September 09, 2004 1:52 PM
To: [REDACTED] (OCA) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

b5

What do you think?

b6

-----Original Message-----

b7C

From: [REDACTED] (OCA) (FBI)

Sent: Thursday, September 09, 2004 8:46 AM

To: FOGLE, TONI M. (INSD) (FBI); THOMPSON, DONALD W. JR (RH)

(FBI)

Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

b5

[REDACTED]

Office of Congressional Affairs
JEH Building Room 7252

b2

[REDACTED]

b6

-----Original Message-----

b7C

From: FOGLE, TONI M. (INSD) (FBI)

Sent: Thursday, September 09, 2004 8:42 AM

To: THOMPSON, DONALD W. JR (RH) (FBI); Hayn, Linda Susan (OCA)

(FBI)

Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

☐ -- can we adjust the language accordingly?

-----Original Message-----

From: THOMPSON, DONALD W. JR (RH) (FBI)

Sent: Wednesday, September 08, 2004 6:01 PM

To: FOGLE, TONI M. (INSD) (FBI)

Subject: RE: Complaints Re: FBI Implementation of Patriot Act

b6

b7C

UNCLASSIFIED

NON-RECORD



b5

-----Original Message-----

From: FOGLE, TONI M. (INSD) (FBI)

Sent: Wednesday, September 08, 2004 1:08 PM

To: THOMPSON, DONALD W. JR (RH) (FBI)

Subject: FW: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED

NON-RECORD



b5

-----Original Message-----

From: ☐ (OCA) (FBI)

Sent: Wednesday, September 08, 2004 12:40 PM

To: FOGLE, TONI M. (INSD) (FBI)

Subject: RE: Complaints Re: FBI Implementation of Patriot Act

b6

b7C

UNCLASSIFIED
NON-RECORD

Toni:

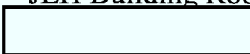


b6
b7C
b5

Thanks.



Office of Congressional Affairs
JEH Building Room 7252



b2

b6

-----Original Message-----

From: FOGLE, TONI M. (INSD) (FBI)^{b7C}

Sent: Friday, September 03, 2004 9:42 AM

To: [redacted] OCA) (FBI)

Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

b5



-----Original Message-----

From: [redacted] OCA) (FBI)

Sent: Friday, September 03, 2004 9:00 AM

To: FOGLE, TONI M. (INSD) (FBI)

Subject: RE: Complaints Re: FBI Implementation of Patriot Act

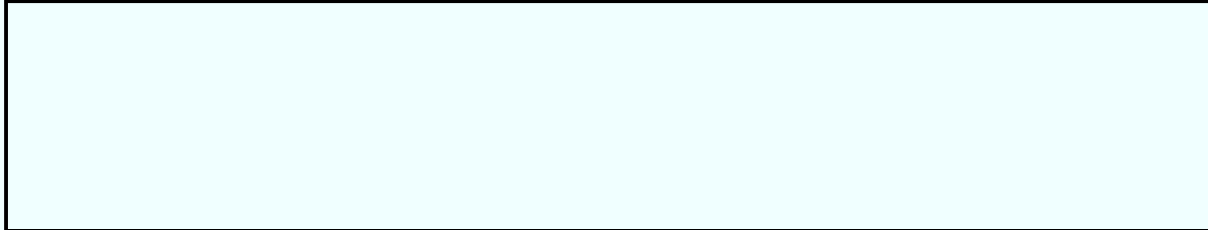
b6

b7C

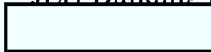
UNCLASSIFIED
NON-RECORD

Toni:

b5



Office of Congressional Affairs
IEH Building Room 7252



-----Original Message-----

b2

From: FOGLE, TONI M. (INSD) (FBI)

b6

Sent: Monday, August 30, 2004 12:45 PM

b7C

To: [redacted] (OCA) (FBI)

Cc: [redacted] (INSD) (FBI)

Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD



b5

-----Original Message-----

From: [redacted] (OCA) (FBI)

Sent: Friday, August 27, 2004 12:29 PM

To: FOGLE, TONI M. (INSD) (FBI)

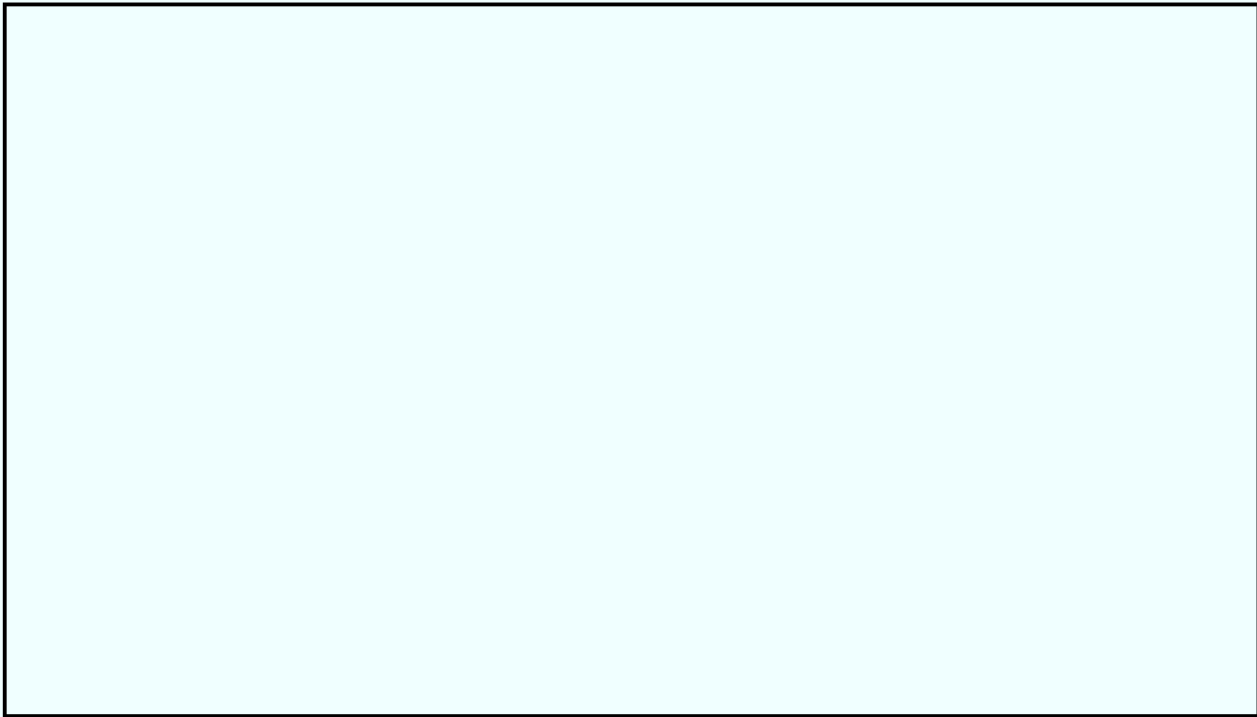
Subject: Complaints Re: FBI Implementation of Patriot Act

b6

b7C

UNCLASSIFIED
NON-RECORD

Toni:



b5

b2

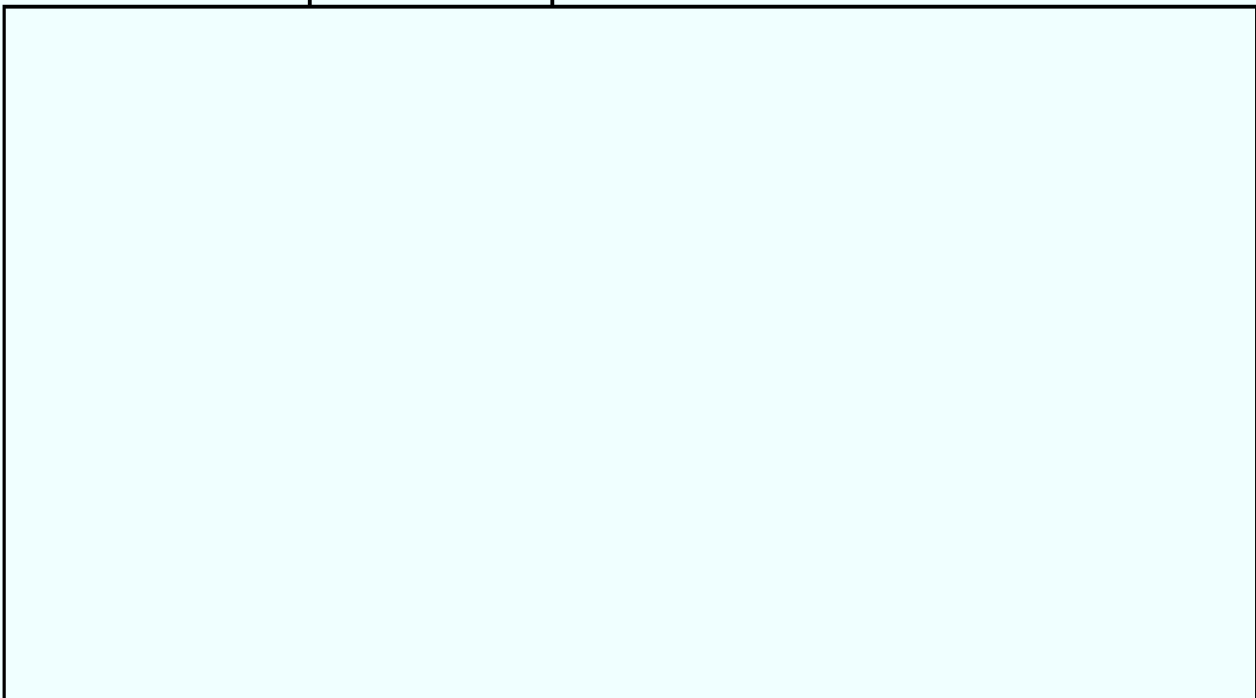
b6

b7C

b5



Office of Congressional Affairs
JEH Building Room 7252



b5

b5

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

MessageFrom: FOGLE, TONI M. (INSD) (FBI)
Sent: Friday, September 03, 2004 9:42 AM
To: [REDACTED] (OCA) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

b6

b5

b7C

-----Original Message-----

From: [REDACTED] (OCA) (FBI)
Sent: Friday, September 03, 2004 9:00 AM
To: FOGLE, TONI M. (INSD) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

Toni:

b5

[REDACTED]
Office of Congressional Affairs
JEH Building Room 7252

b2

b6

b7C

-----Original Message-----

From: FOGLE, TONI M. (INSD) (FBI)
Sent: Monday, August 30, 2004 12:45 PM
To: [REDACTED] (OCA) (FBI)
Cc: [REDACTED] (INSD) (FBI)
Subject: RE: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED
NON-RECORD

[Redacted]

b5

-----Original Message-----

From: [Redacted] (OCA) (FBI)

b6

Sent: Friday, August 27, 2004 12:29 PM

b7C

To: FOGLE, TONI M. (INSD) (FBI)

Subject: Complaints Re: FBI Implementation of Patriot Act

UNCLASSIFIED

NON-RECORD

Toni:

[Redacted]

b5

[Redacted]

[Redacted]

[Redacted]

b2

Office of Congressional Affairs

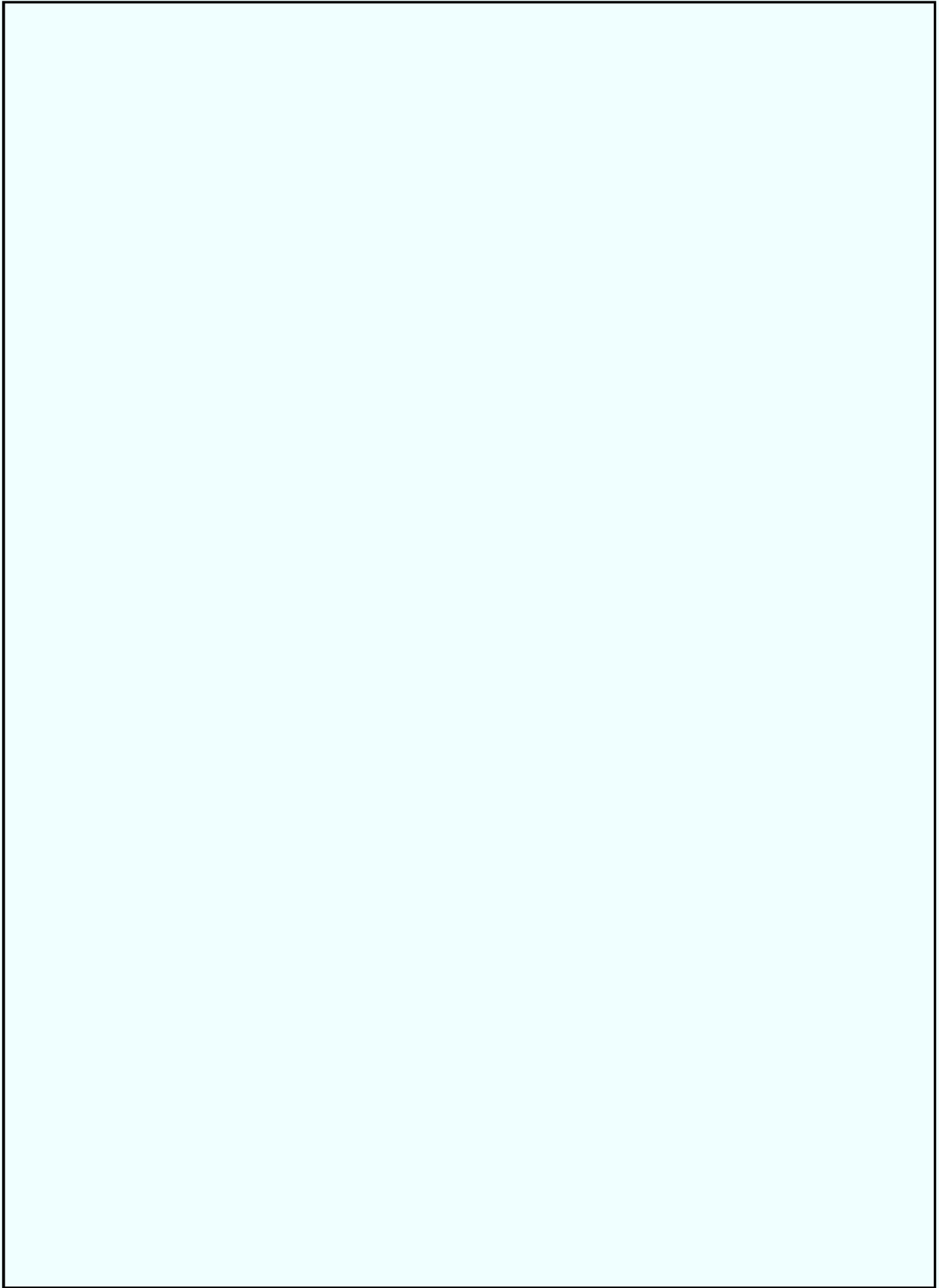
b6

JEH Building Room 7252

b7C

[Redacted]

b5



b5

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

Questions for Investigative Law Unit

8. Office of the General Counsel (OGC). At the hearing on May 20, you stated that the Department of Defense had not, to date, referred any prisoner abuse cases involving military contractors to DOJ. The next day, DOJ announced that it had received such a referral the day before and that it had "opened an investigation into the matter."

a. At what time on May 20 did DOJ receive the referral from DOD?

Response:

b. When did you first learn about that referral?

Response:

c. Is the FBI conducting this investigation and, if not, what investigating body is?

Response:

b5

9. OGC. At the hearing, you noted that the CIA had referred a prisoner abuse case to DOJ, but that the investigation was being conducted by the CIA Inspector General and not the FBI. Has the FBI become involved in that investigation since the hearing? If not, what investigating body or bodies are involved?

Response:

56. Has a final decision been made as to whether prior approval is mandatory for visiting a public place or attending a public event to detect or prevent terrorist activity?

Response:

b5

66. Has the FBI implemented any new professional rules of conduct or code of ethics policies that provide safeguards against FBI abuse of its PATRIOT Act authorities? What, if any, internal or disciplinary punishments are in place for abuses by employees?

Response:

80. The authority to arrest and detain a person whose "testimony . . . is material in a criminal proceeding" is set forth at 18 U.S.C. 3144, "Release or detention of a material witness." The following questions pertain to the use of that provision in counterterrorism investigations and prosecutions during the period of time from September 11, 2001 to the present.

a. In how many cases have the authorities of 18 U.S.C. 3144 been used?

b. How many individuals are currently detained under the authority of 18 U.S.C. 3144?

c. In how many cases where the authority of 18 U.S.C. 3144 has been used has the individual arrested and detained in fact testified in "a criminal proceeding."

d. 18 U.S.C. 3144 prohibits the detention of any individual where "testimony of such witness can adequately be secured by deposition." In how many cases where the authority of 18 U.S.C. 3144 has been used has a deposition been taken and the witness released?

e. In how many cases in which an individual has been arrested or detained pursuant to 18 U.S.C. 3144 has the witness been subsequently charged with a crime?

f. In how many cases in which an individual has been arrested or detained pursuant to 18 U.S.C. 3144 has the witness be subsequently transferred to the custody of the Department of Defense? Please describe the facts and circumstances of each such case.

g. In how many cases in which an individual has been arrested or detained pursuant to 18 U.S.C. 3144 has the witness be subsequently transferred to the custody of a foreign government? Please describe the facts and circumstances of each such case.

Response

--

h. What procedures and safeguards are in place to ensure that the authorities of 18 U.S.C. 3144 are not being used for purposes of preventive detention, or to hold individuals suspected of criminal activity without charging them with the commission of a crime?

b5

Response:

--

i. What written policies or directives of the Department of Justice or the Federal Bureau of Investigation govern the application of the authorities set forth in 18 U.S.C. 3144?

b5

Response:

81. In briefs filed with the Supreme Court in the matter of Padilla v. Rumsfeld, as well as in related cases and in public statements, the President and the Attorney General have asserted that the President, in his capacity as Commander-in-Chief may detain individuals, including United States citizens, as "enemy combatants." The following questions pertain to the exercise of this authority during the period from September 11, 2001 to present.

a. What role has the Federal Bureau of Investigation played in the arrest, detention, and interrogation of individuals held in custody pursuant to this authority as "enemy combatants?"

Response: (Reassigned to CTD)

b. How many individuals have been arrested or detained pursuant to this authority?

c. How many United States citizens have been arrested or detained pursuant to this authority?

d. How many United States persons, as defined in Executive Order 12333, Section 3.4(i), and excepting United States citizens, have been arrested or detained pursuant to this authority?

Response:

b5

e. What rules, procedures or practices govern the conditions of confinement and the methods of interrogation used in cases where an individual has been arrested or detained pursuant to this authority?

b5

Response:

83. Sections 201 and 202 of the USA-Patriot Act added a number of offenses to the "predicate offense list" applicable to criminal wiretaps pursuant to Chapter 119 of Title 18. The following question pertains to the time period since the passage of the USA-Patriot Act, October 26, 2001.

a. In how many cases has have the newly-added predicate offenses been used to support an application for a criminal wiretap under the authority of Chapter 119 of Title 18?

Response:

b. In how many such cases has the newly-added predicate offense been the only predicate offense asserted as the basis for the warrant, i.e., where a warrant could not have been lawfully issued but for the passage of the additional criminal predicates?

b5

Response:

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute, including the addition of predicate crimes, which the Congress should consider?

Response: Sections 201 and 202 of the USA Patriot Act are currently scheduled to expire at the end of 2005.

b5

87. Section 209 of the USA-Patriot Act clarified the law with regard to the applicability of criminal search warrants to voice mail. This question pertains to application of this provision since its passage.

a. How many such search warrants have been issued since

passage of this act?

Response:

--

b5

b. In such cases, have there been any instances in which a wiretap, as opposed to a search, warrant would not have been supported by the facts asserted in support of the search warrant.

Response: This information is unavailable for the same reasons stated above. It is clear, however, that the requirements to obtain an federal wiretap are considerably greater than those for a search warrant.

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

--

b5

b5

95. Section 225 of the USA-Patriot Act provides immunity for those who aid in the execution of a FISA order. Has such immunity been invoked?

Response: No; with respect to FBI investigations, immunity has not been claimed under this section in either the civil or criminal context.

Brandon Mayfield Fingerprint Identification and Detention

101. On May 24th, a federal court dismissed the material witness proceeding against Brandon Mayfield, an attorney and former U.S. Army officer. In written submissions to the court and in public statements the FBI has admitted that the fingerprint of Mayfield was mistakenly matched to a fingerprint recovered at the scene of the May 11, 2004, Madrid train bombing.

d. According to court records, no criminal charges were ever filed against Mayfield. Instead, he was detained as a material witness. Why was Mayfield held as a material witness and not charged with any criminal conduct?

Response:

b6
b7C

Use of the USA PATRIOT Act

102. In October 2003, the Department reported that as of April

1, 2003, it had sought, and courts had ordered, delayed notice warrants 47 times.

a. As of the date of your response to these questions, or some reasonable recent date, how many times has the Department sought and received authorization to execute a delayed notification search since enactment of the PATRIOT Act?

Response: The number of delayed notice search warrants reported in April 2003 was compiled by the Executive Office of United States Attorneys (EOUSA) through a field survey of U.S. Attorney's Offices. It is our understanding that EOUSA is currently updating that figure with another survey. When that figure is made known to the FBI, it will be provided.

b. How many of the delayed notification warrants issued since passage of the PATRIOT Act were granted because contemporaneous notification would have "seriously jeopardized an investigation"? For each such delayed notice warrant, please describe how granting contemporaneous notice would have seriously jeopardized the investigation and please indicate whether seriously jeopardizing the investigation was the sole basis or one of multiple grounds for delaying notice.

c. How many of the delayed notification warrants issued since passage of the PATRIOT Act were granted because contemporaneous notification would have "unduly delayed a trial"? For each such delayed notice warrant, please describe how requiring contemporaneous notice would have unduly delayed a trial and please indicate whether unduly delaying a trial was the sole basis or one of multiple grounds for delaying notice.

Response (b. and c.):

--

b5

d. How many of the delayed notice warrants were issued with a (i) seven-day or less delay; (ii) 8 to 30 day delay; (iii) 31

to 60 day delay; and (iv) time period of 61 days or more and what were those time periods?

e. How many of the delayed notification warrants issued since the PATRIOT Act was passed were used in non-terrorism criminal matters?

f. Please provide the case name, docket number, and court of jurisdiction for each case in which a delayed notice warrant was issued since enactment of the PATRIOT Act.

Response

--

b5

Message From: BOWMAN, MARION E. (OGC) (FBI)

Sent: Tuesday, August 31, 2004 5:53 AM

To: [REDACTED] (OCA) (FBI)

b6

Cc: [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (OGA); KELLEY,

b7c

PATRICK W. (OGC) (FBI)

Subject: RE: PLEASE DELETE LAST MESSAGE. NSLB RESPONSES WITH CTD INPUT

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

I'll do what I can, but OGC is not the place to answer most of this. 84b(i) and 84c look fine to me, but OGC is not in the loop for the activity represented. I don't have the questions so don't know what the others are (I'll check with [REDACTED] here), but, as you know, we don't run cases either so what the field does is often unknown to us, or anyone at HQ.

-----Original Message-----

From: [REDACTED] (OCA) (FBI)

b6

Sent: Monday, August 30, 2004 5:37 PM

b7c

To: BOWMAN, MARION E. (OGC) (FBI)

Cc: [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (OGA); KELLEY,

PATRICK W. (OGC) (FBI)

Subject: RE: PLEASE DELETE LAST MESSAGE. NSLB RESPONSES WITH CTD INPUT

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Spike. Thanks. I had previously received much of this, but this does fill in a few gaps.

Here's where we stand.

1. This document provides the following answers for the first time.

84b(i) (which has several subparts)

84c (which has several subparts)

I need approval of these answers by a DAD (or equivalent) or higher. Do we have a demonstration that these were approved by [REDACTED] If not, could you review them and forward to me your approval (email is fine)?

b6

b7c

2. I still need responses to the following:

88a, b, d

91a, b

93a, c

A couple of these questions (such as # 88a) request numbers of cases, which I understand we may not keep. If you let me know that, I can try to deal with those. I do, however, need the rest of the responses. For example, while 88a asks for the number of cases in which we've used Section 212 of the Patriot Act (which we may not be able to answer), 88b asks for cases in which

we needed Patriot Act authority for a reason other than time constraints, and 88d asks if we want changes to 212.

I know inflicts incredible pain and agony. Does it help that I find this painful as well?

[REDACTED]

Office of Congressional Affairs
JEH Building Room 7252

b2

[REDACTED]

b6

-----Original Message-----

b7c

From: BOWMAN, MARION E. (OGC) (FBI)

Sent: Monday, August 30, 2004 4:47 PM

To: [REDACTED] (OCA) (FBI)

Cc: [REDACTED] (OGC) (FBI) [REDACTED] (OGC) (OGA); KELLEY,
PATRICK W. (OGC) (FBI)

Subject: FW: PLEASE DELETE LAST MESSAGE. NSLB RESPONSES WITH CTD INPUT

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

I thought these had been forwarded already, but in case not, here they are.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

DATE: 12-08-2005
CLASSIFIED BY 65179 DMH/DD
REASON: 1.4 (C)
DECLASSIFY ON: 12-08-2030

~~Secret~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

QUESTIONS FOR THE RECORD FROM DIRECTOR'S 5/20/04 SENATE HEARING
NSLB RESPONSES

28. OGC. During the hearing, Senator Grassley asked you about the retroactive classification of information provided by the FBI to Committee staff related to a whistleblower who previously worked for the FBI translation program. I share Senator Grassley's concern that this order is unrealistic. A great deal of information regarding the whistleblower's claims, including the FBI's corroboration of many of the problems she raised, has been in the public record for more than two years. I appreciated your statement that the retroactive classification order was not intended to place a gag on Congress. However, the notice received by staff members of the Judiciary Committee was very vague, referring only to "some" information conveyed in the briefings. If state secrets are truly implicated by something that was said in an unclassified briefing two years ago, the FBI should provide very specific instructions to current and former staff on what information must be kept secret. Will you instruct your staff to provide more specific information to relevant staff about what, exactly, from the 2002 briefings is classified and what is not?



b5

33. OGC. You testified that, prior to the PATRIOT Act, "if a court-ordered criminal wiretap turned up intelligence information, FBI agents working on the criminal case could not share that information with agents working on the intelligence case." Please state specifically what law or laws prevented such information-sharing prior to PATRIOT, and whether a court could authorize such information-sharing, regardless of any such law or laws?

Response: Prior to the changes brought about by the Patriot Act, Title 18 Section 2517 was interpreted to solely authorize the sharing of intercepted wire, oral, or electronic

~~SECRET~~

~~SECRET~~

communications for criminal law enforcement purposes without the need to obtain a court order. Sharing intercepted information for foreign intelligence purpose required a court order and, based upon the statutory language, it was unclear whether a judge would sign an order. The changes to the Patriot Act clearly allow the sharing of foreign intelligence information developed during a court-ordered criminal wiretap with the agents working intelligence cases.

34. OGC. You further testified that, prior to the PATRIOT Act, "information could not be shared from an intelligence investigation to a criminal investigation." Please state specifically what law or laws prevented such information-sharing prior to PATRIOT?

Response: Prior to the Patriot Act, there were procedures for sharing information between intelligence investigators and criminal agents and prosecutors, but they were difficult, burdensome and usually resulted in less than fulsome sharing. For example, the FISA statute was interpreted to require a "primary purpose" of gathering intelligence in order to secure a FISA Court order. Because of this interpretation of the FISA statute, the Department of Justice and the FISA Court required that certain procedures be followed in order to share intelligence with criminal investigators and prosecutors.

b5

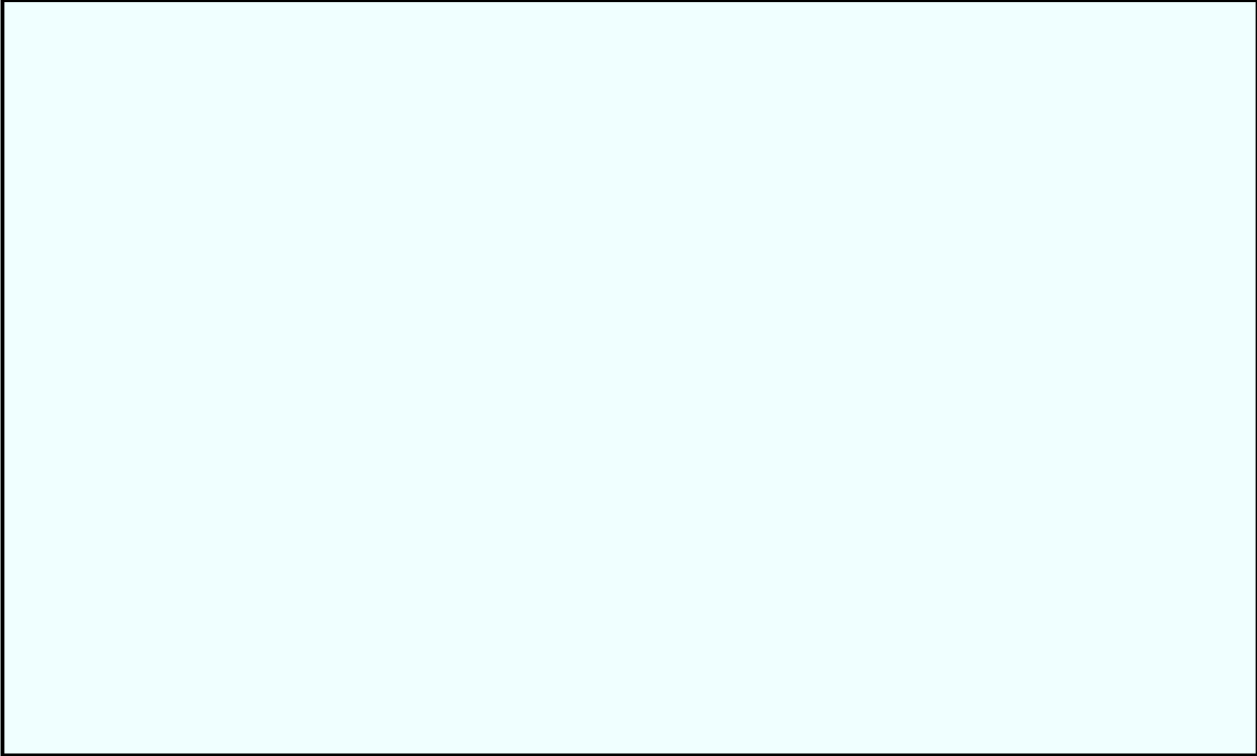
For additional information, see the answer to question 35.

35. OGC. In his statement to the 9/11 Commission, the Attorney General blamed the creation of the so-called "wall" between criminal investigators and intelligence agents on a 1995 memorandum authored by a senior official in the Reno Justice Department, now a member of the 9/11 Commission.

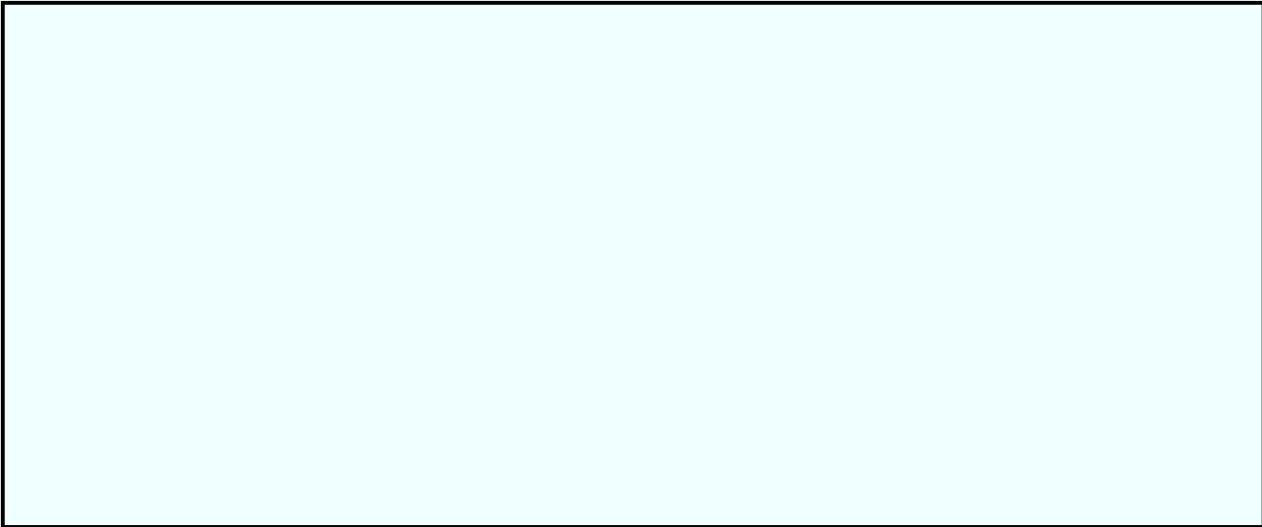
a. Do you agree that the architecture of the wall was in place long before 1995, having its genesis in established legal doctrine dating from 1980? If not, how do you explain the extensive discussion of this issue in the one and only reported opinion of the FISA Court of Review, decided on November 18, 2002?

~~SECRET~~

~~SECRET~~



b5



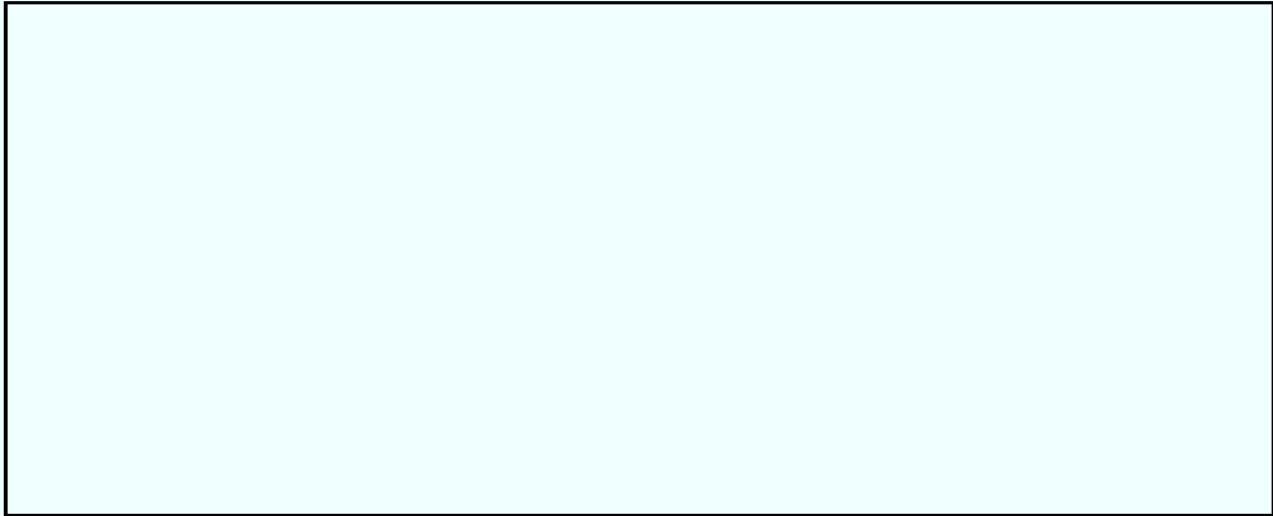
b5



b5

~~SECRET~~

~~SECRET~~



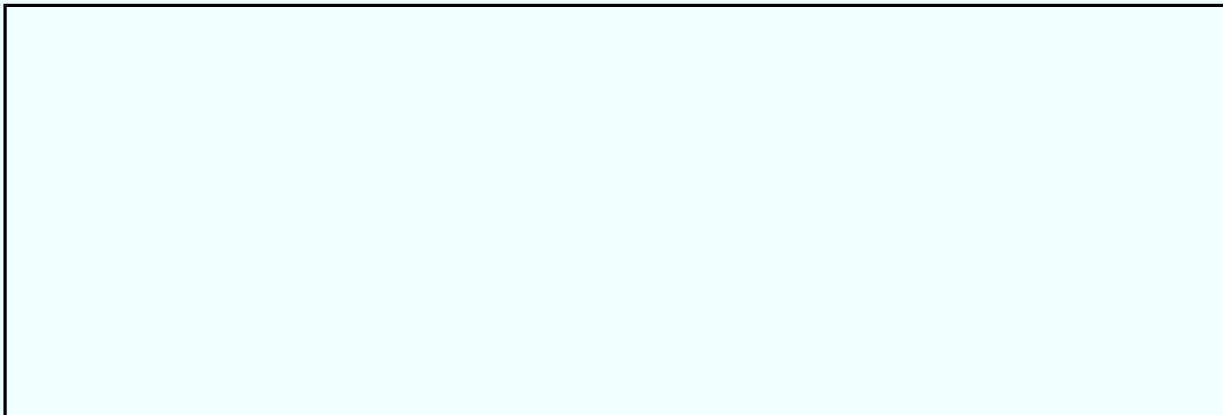
b5

How did the FBI handle information-sharing between criminal investigators and intelligence agents before 1995?



b5

b. Do you agree that the Gorelick memo established proactive guidelines amidst a critically important terrorism prosecution to *facilitate* information sharing.



b5

~~SECRET~~

~~SECRET~~

b5

55. CTD. (Follow-up to Leahy 15) What specific policy changes have you made in response to the Inspector General's report on 9/11 detainees?

OCA Note: To assist CTD in responding, we note that, in response to a Question for the Record regarding a 9/11 Detainee hearing, the FBI indicated that DOJ and DHS had signed a memorandum of understanding (MOU) related to information sharing and, as recommended by the Inspector General, the FBI was working with DOJ to draft an MOU governing the detention of aliens of interest to the FBI. We also indicated that we were working with DHS to establish criteria and procedures for future investigations of alien detainees, including circumstances where a large number of aliens with potential ties to terrorism are detained.

Response: The DOJ and DHS have signed a memorandum of understanding (MOU) relating to information sharing and the FBI is working with DOJ to draft an MOU governing the detention of aliens of interest to the FBI. DOJ is still working with DHS to draft an MOU to establish criteria and procedures for future investigations of alien detainees of national security interest. With respect to other policy changes, the FBI has worked to establish the Terrorist Screening Center (TSC) and TTIC, which will substantially improve the FBI's ability to obtain information about alien detainees from various agencies and process this information in a timely fashion. The FBI continues to work with the National Security Law Division, ICE, to review alien detainee cases of national security interest on a case-by-case basis.

58. OGC. (Follow-up to Leahy 18A) When will the FISA Management System (FISAMS) be fully operational? With whom is the contract for development of FISAMS? How much will it cost and what funds are being used to pay for it?

Response: The FISA Management System (FISAMS) became operational at the end of January 2004. The FBI trained the largest 13 FBI field offices on the system. These 13 offices are currently processing their FISA requests through the FISAMS,

~~SECRET~~

~~SECRET~~

extent permitted by the Constitution and the laws of the United States. In addition, as the Acting Deputy Attorney General explained in his November 20, 2003 Memorandum to the Inspector General in response to the Inspector General's report, the FBI will work with DHS to establish criteria for future investigations (the specific criteria will depend on the nature of the national emergency). [REDACTED] b5

[REDACTED] In addition, the creation of TSC and TTIC will greatly improve the FBI's ability to gather information concerning aliens of national security interest and work with the appropriate federal agencies to determine the best means of averting any national security threat, whether through criminal or immigration proceedings. Other initiatives, such as the Foreign Terrorist Tracking Task Force and the National Joint Terrorism Task Force have assisted in permitting better information flow with our law enforcement counterparts and will improve the handling of such cases. [REDACTED] b5

82. OGC. Title 18 Section 3103a, as amended by Section 213 of the USA-Patriot Act (P.L. 107- 56), provides authority for delaying notice of the execution of search warrants. The following question pertains to the use of the authority provided in this section in investigations or prosecutions related to terrorism during the period of time from September 11, 2001 to the present.

a. In how many such cases has the authorities to delay notification been used?

b. In how many such cases has the authority added by Section 213(b)(1), which allows a delay where "the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result" been used? Please describe the circumstances in each of these cases.

c. In how many such cases has the authority set forth in 18 U.S.C. 2705(E), which provides for delay in cases which would "otherwise seriously jeopardize an investigation or unduly delay a trial" been used? Please describe the circumstances in each of these cases?

~~SECRET~~

~~SECRET~~

b5

84. Sections 203(b) and 203(d) of the USA-Patriot Act provide specific authority for the provision of intelligence information acquired in the course of a criminal investigation to elements of the Intelligence Community. Section 901 of the same act makes such disclosure in most cases mandatory. The following questions pertain to the implementation of these sections.

a. OGC. Section 203(c) of the USA-Patriot Act requires the Attorney General to "establish procedures for the disclosure for the disclosure of information" as provided for in Section 203. Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

Response to Q84 a: On September 23, 2002, the Attorney General promulgated guidelines that established the procedures for disclosure of information under Section 203 of the Patriot Act. A copy of the guidelines is attached. The Office of the General Counsel issued an EC advising all Divisions of the procedures. A copy of the EC is attached.

b. OGC. Section 203(b) specifically provides authority "to share electronic, wire, and oral interception information" where such information is foreign intelligence information. What is the method for disseminating such information to the Intelligence Community?

Response: This information may be disseminated in any format deemed appropriate for the particular circumstances. [As to the sub questions below, OGC does not have information pertaining to electronic intelligence reports and refers OCA to CTD.]

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203 (b) material?

(1) If so, how many such reports have been

~~SECRET~~

issued?

~~SECRET~~

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

c. OGC. Section 203(d), the so-called "catch-all" provision, provides a general authority to share foreign intelligence information with the Intelligence Community. What is the method for disseminating such information to the Intelligence Community?

Response: The information may be disseminated in any format deemed appropriate for the circumstances. [OGC would refer the remaining sub-parts to CTD for a response as to how they are disseminating this information.]

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(d) material?

(1) If so, how many such reports have been issued?

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

d. OGC. Section 905(c) of the USA-Patriot Act requires the Attorney General to "develop procedures for the administration of this section. . . ." Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

Response: On September 23, 2002, the Attorney General promulgated guidelines that established procedures for the disclosure of information under Section 905(a) of the USA-Patriot Act. A copy of the procedures is attached as well as the Office of the General Counsel's EC advising all Divisions of these procedures. The Attorney General also promulgated guidelines under Section 905(b) of the USA Patriot Act (see attached). OGC is not aware of procedures established under Section 905(c) of

~~SECRET~~

~~SECRET~~

the USA-Patriot Act and would refer this question to DOJ.

e. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 203 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

f. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

b5

[redacted] OGC strongly believes that Section 203 (b) and (d) should not be allowed to expire on December 31, 2005. The changes brought about by the Patriot Act have significantly increased the ability of the FBI to share information. [Note: DOJ has provided or is in the process of providing examples of how the Patriot Act has been an asset to our investigations and why the sunset provisions should not sunset. We refer OCA to the DOJ for these examples.]

85. Sections 206 of the USA-Patriot Act, the so-called "roving wiretap" provision, permits the issuance of a FISA warrant in cases where the subject will use multiple communication facilities. This question pertains to the implementation of this section during the time period since the passage of the USA-Patriot Act, October 26, 2001.

Response:

a. How often has this authority been used, and with what success?

b5

~~SECRET~~

~~SECRET~~

b. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to the FISA?

b5

Response: FBI intelligence products are an important vehicle for the dissemination of both FISA-derived and non-FISA foreign intelligence information, but not the only one. [REDACTED]

More specifically, the FBI shares many forms of foreign intelligence with other members of the Intelligence Community, [REDACTED]

b5 [REDACTED] through direct classified and unclassified dissemination and through websites on classified Intelligence Community networks. The FBI also shares intelligence with representatives of other elements of the Intelligence Community who participate in Joint Terrorism Task Forces (JTTFs) in the United States or with whom the FBI collaborates in activities abroad. FBI intelligence products shared with the Intelligence Community include Intelligence Information Reports (IIRs), Intelligence Assessments, and Intelligence Bulletins.

The FBI also disseminates intelligence information through Law Enforcement Online (LEO), a virtual private network that reaches federal, state, and law enforcement agencies at the Sensitive But Unclassified (SBU) level. LEO makes finished FBI intelligence products available, including Intelligence Assessments resulting from analysis of criminal, cyber, and terrorism intelligence. [REDACTED]

b5 [REDACTED] Intelligence Information Reports also are available on LEO at the Law Enforcement Sensitive classification level. The FBI also recently posted the requirements document on LEO, which provided state and local law enforcement a shared view of the terrorist threat and the information needed in every priority area.

(i) If so, how many such reports have been issued?

Response: In the past two years the FBI's Counterterrorism

~~SECRET~~

~~SECRET~~

Division's Terrorism Reports and Requirements Section has disseminated 76 intelligence information reports (IIRs) containing information derived from FISA-authorized surveillance and/or search. (Statistics are not maintained in such a way that would enable us to say whether any of the FISA-derived information in the reports was obtained using "roving authority.") Other FBI Divisions have also issued reports containing FISA-derived information. For example, the Cyber Division has written a total of 24 electronic information reports containing FISA-derived information.

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response: The Office of Intelligence promulgated the FBI's Intelligence Information Report Handbook on 9 July. The Handbook establishes the first comprehensive FBI-wide guide for the format and content of raw intelligence reports. The Office of Intelligence is working to develop evaluation guidelines based, in part, on the criteria established in the Handbook for the types of information to be reported and shared with our law enforcement and intelligence community partners, [REDACTED]

b5

In addition, the FBI's Inspection Division has established evaluation criteria for the value of human source reporting, [REDACTED] [REDACTED] access and responsiveness to local FBI field office, FBI program and national intelligence requirements. The Office of Intelligence is developing guidelines to use this same criteria as a means of evaluating the value of raw intelligence. Initial discussions on this issue have been held with representatives from the Counterintelligence, Counterterrorism, Criminal and Cyber Divisions. The results of these discussions are being incorporated into evaluation guidelines.

c. Some have read this section as providing for surveillance in cases where neither the identity of the subject or the facility to be used is known -- in effect, allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversation of an unknown person. Is this the reading of the statute being adopted by the Federal Bureau of Investigation and the Department of Justice? If not, please provide your interpretation of this authority.

~~SECRET~~

~~SECRET~~

Response: No, the FBI does not interpret the statute as allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversations of an unknown person. In order to make a showing of probable cause, the FISA statute requires a statement of the facts and circumstances relied upon by the applicant for surveillance to justify the belief that: (1) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and, (2) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. Thus, the FISA statute does not permit coverage to be authorized, with or without the "roving wiretap" provision, to allow for surveillance against all persons in a particular geographic area. The FBI has interpreted the "roving" authority as permitting the FBI to request that the Foreign Intelligence Surveillance Court issue a "generic" secondary order, along with specified orders, for a specifically identified FISA target, that the FBI could serve in the future on the unknown (at the time the order is issued) cell phone carrier, Internet service provider, or other communications provider, if the target rapidly switches from one provider to another. The roving wiretap order still requires that a federal law enforcement agent swear in a detailed affidavit to facts establishing probable cause, and still requires a court to make a finding of probable cause before issuing the order. The roving order has the additional requirement of a judge's approval to monitor more than one telephone. But now, each time a target changes his cellular telephone, instead of going through the lengthy application process, government agents can use the same order to monitor the target. This will allow the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the Court for a new secondary order. The FBI views this as a vital and necessary tool to counter certain targets who engage in such actions as a deliberate means of evading surveillance.

(i) Have any briefs been filed with the Foreign Intelligence Surveillance Court on this subject? If so, please provide copies of such briefs to the Committee.

Response: The FBI has filed no such briefs on this subject.

d. Inspection Division

e. Based upon the application of this provision of law during

~~SECRET~~

~~SECRET~~

the period since its passage, are there changes to this statute which the Congress should consider?

Response: No, we request only that the provision be preserved.

86. Section 207 of the USA-Patriot Act extends the time limits provided in the FISA which govern surveillance against agents of a foreign power.

a. Has the Federal Bureau of Investigation or the Department of Justice conducted any review to determine whether, and if so, how many, personnel resources have been saved by this provision? If so, please provide the results to the Committee.

b5

b. Have there been any cases where, after the passage of the now-extended deadlines it was determined, either by the Department of Justice, the Federal Bureau of Investigation or the Foreign Intelligence Surveillance Court, that surveillance should have been terminated at an earlier point because of the absence of a legally required predicate.

Response: None of which the FBI is aware.

c. Inspection Division

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response: None at this time.

89. Section 214 of the USA-Patriot Act permits the use of FISA pen register/trap & trace orders with respect to electronic communications, and eliminates the requirement that such use be only in the context of a terrorist or espionage investigation. This question pertains to application of this provision since its passage, and to all instances, not only terrorism investigations.

a. OGC. In how many cases has this authority been used?

~~SECRET~~

~~SECRET~~

b5

(i) How many of such cases were terrorism-related?

b5

b. OGC. Of the cases in which such authority was used, in how many was a subsequent application for a full surveillance order made pursuant to the FISA, or Chapter 19 of Title 18?

Response: OGC does not have a way to determine how many pen registers evolved into full FISA's.

c. Inspection Division. Has the Intelligence Community, Department of Justice, or Federal Bureau of Investigation developed regulations or directives defining the meaning of non-content communications? If such regulations or directives have been issued, please provide copies to the Committee.

d. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response: Please see answer to Question 85.

90. Section 215 of the USA-Patriot act authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application

~~SECRET~~

~~SECRET~~

of this provision since its inception.

a. OGC. How many times has this authority been used, and with what success?

b. OGC. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.

c. OGC. In your testimony you compared this provision with existing authority in the criminal context, noting that records such as library records are subject to a grand jury subpoena. However, in criminal cases the propriety and lawfulness of subpoenas are to some extent tested in the adversary process of a trial - how, in the context of the FISA, does such a check occur?

d. OGC. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

(i) With respect to the potential applicability of this section to libraries and bookstores, there has been some concern that the mere prospect of use of the statute has a "chilling effect" on the use of these facilities. Can this chilling effect be minimized, if not eliminated, by incorporating a higher threshold for use in the limited context of libraries and bookstores? If not, why not?

e. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

f. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation

~~SECRET~~

~~SECRET~~

received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

g. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

b1
b2
b7E

Response:

a

[Redacted]

(S)

b

[Redacted]

(S)

[Redacted]

b5

[Redacted]

(U)

b2
b5
b7E

[Redacted]

[Redacted]

~~SECRET~~

~~SECRET~~

b2

b7E

(U)

b5

(U)

(S)

b1

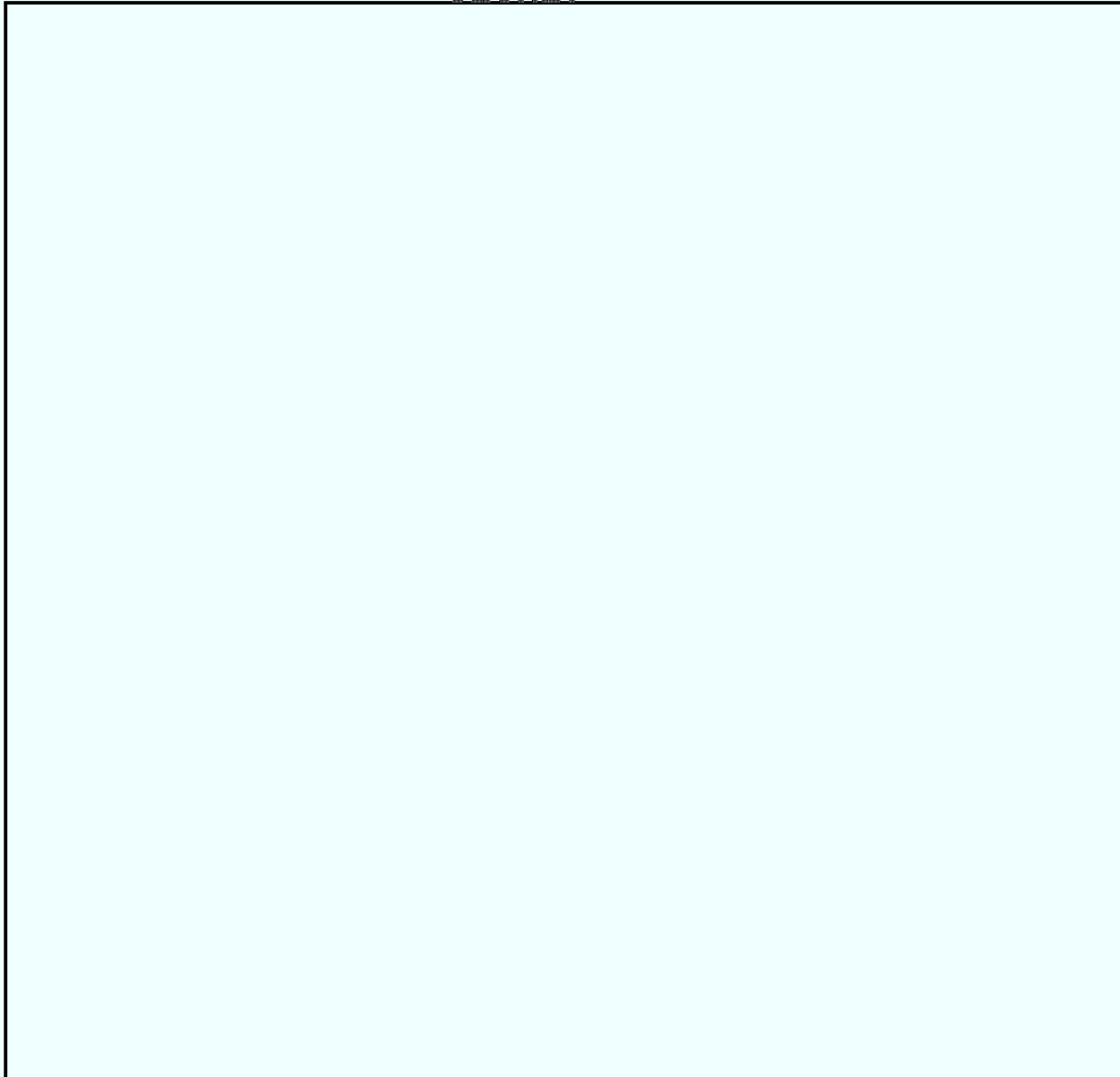
b2

b7E

b5

~~SECRET~~

~~SECRET~~



b5

e. QUESTION RE "ELECTRONIC INTELLIGENCE REPORTS" - PLEASE REFER TO CTD.

f. FOR INSPECTION DIVISION



b5

92. Section 218 of the USA-Patriot Act created the so-called "significant purpose" test for applications pursuant the FISA, clarifying the law to recognize that in many cases such surveillance may implicate both a law enforcement and an intelligence interest. This question pertains to the implementation

~~SECRET~~

~~SECRET~~

of this provision since its passage.

a. OGC. Please provide the Committee with specific examples, in unclassified form if possible, of cases in which both law enforcement and intelligence interests were "significant."

b. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 218 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

c. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

b5

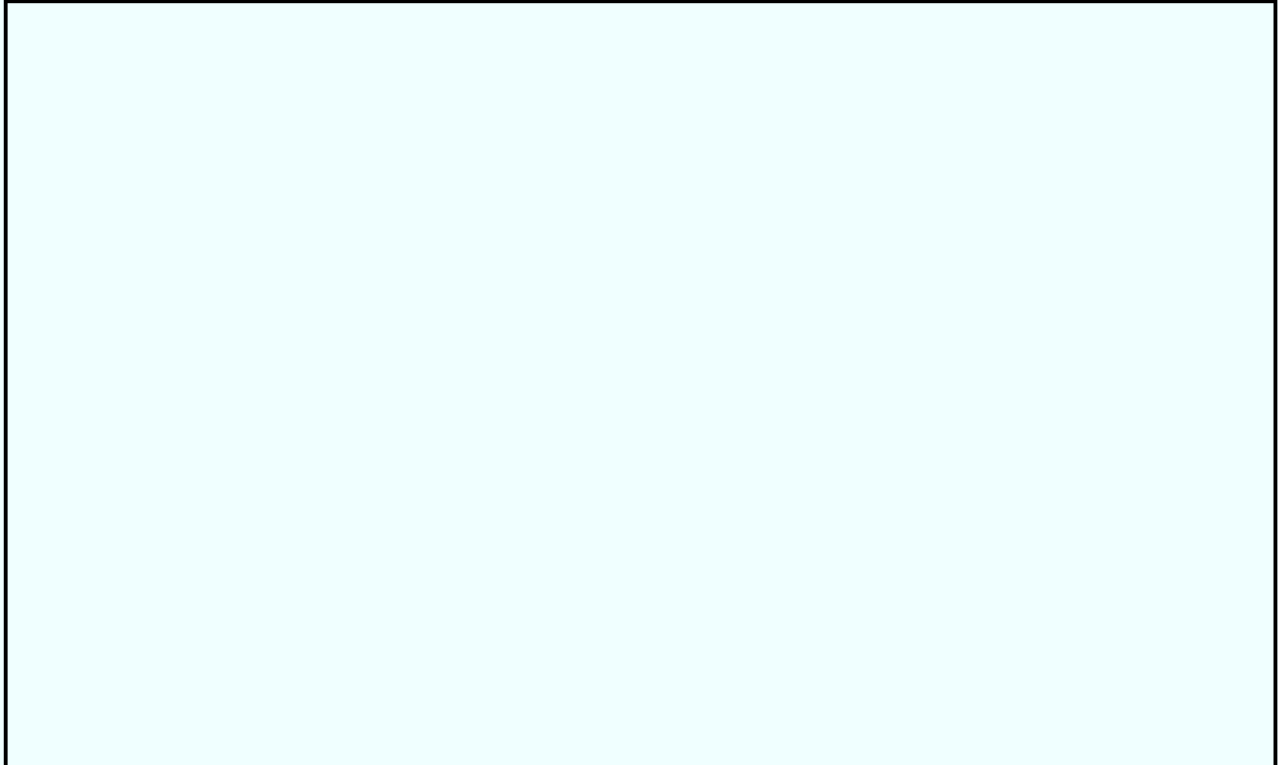
b5

~~SECRET~~

~~SECRET~~



b5

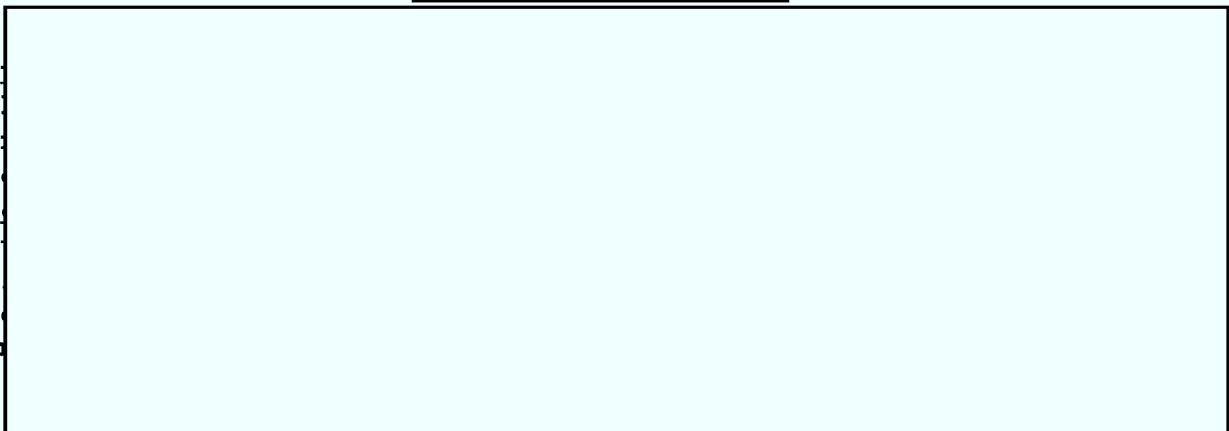


b5

b1

b7A

(S)



b5

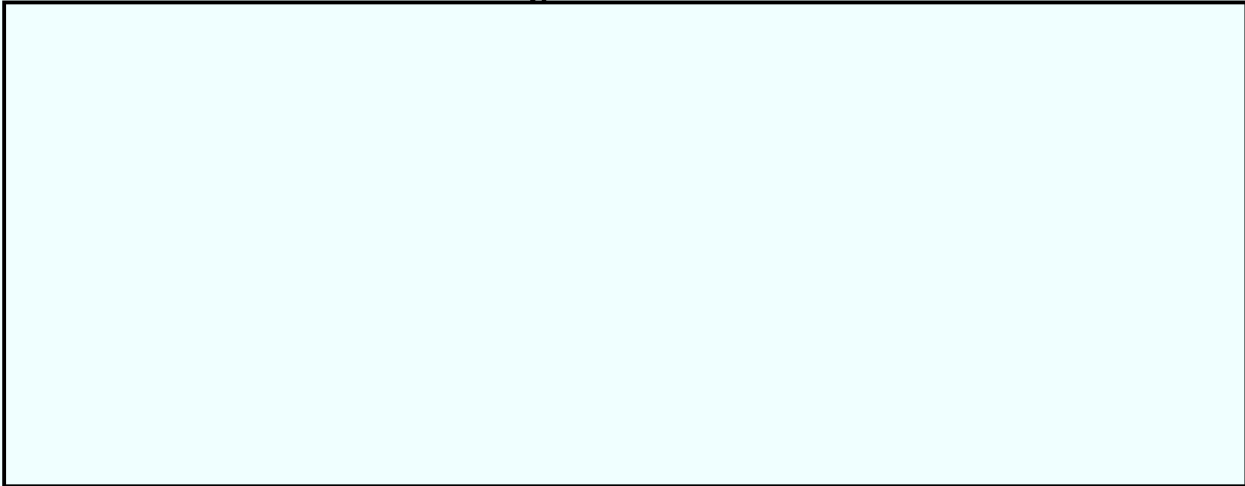
b7A

b6

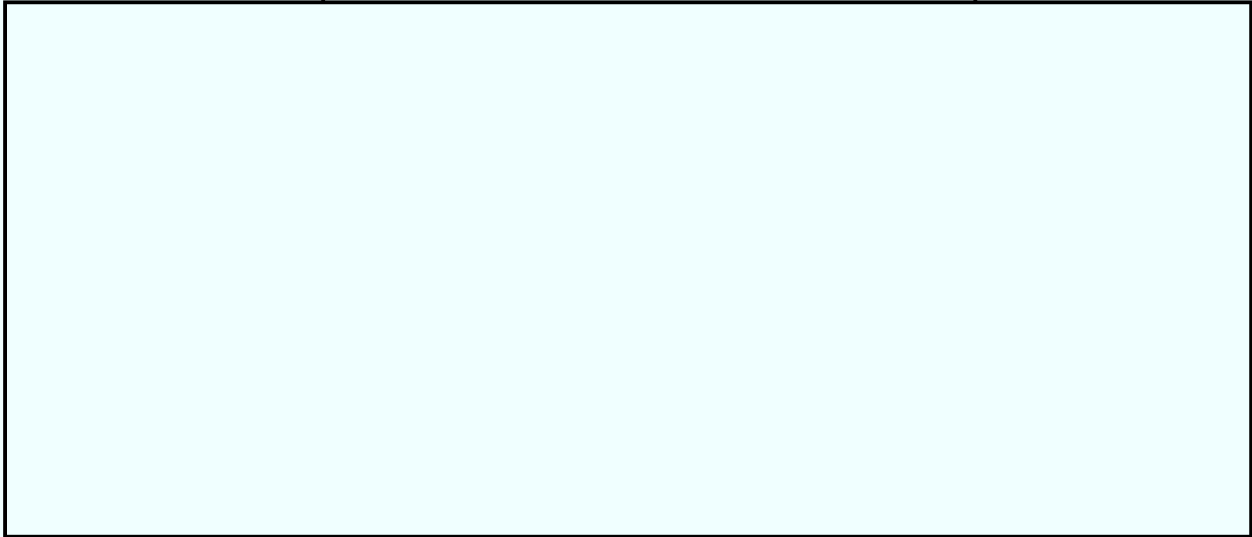
b7C

~~SECRET~~

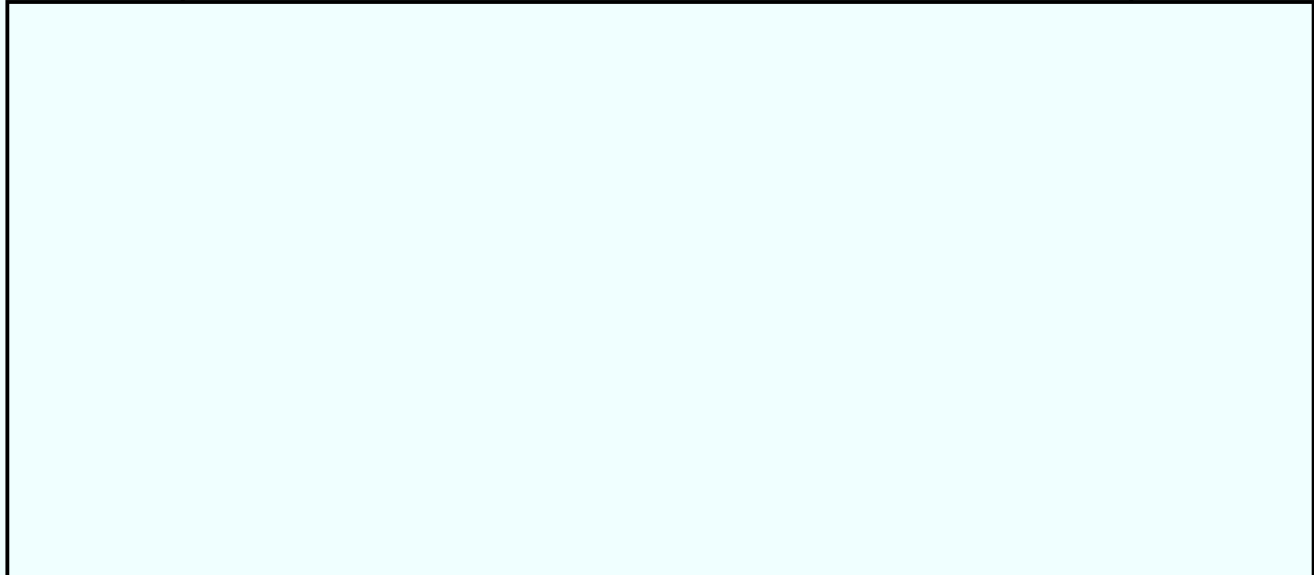
~~SECRET~~



b5
b6
b7C
b7A



b5
b7A

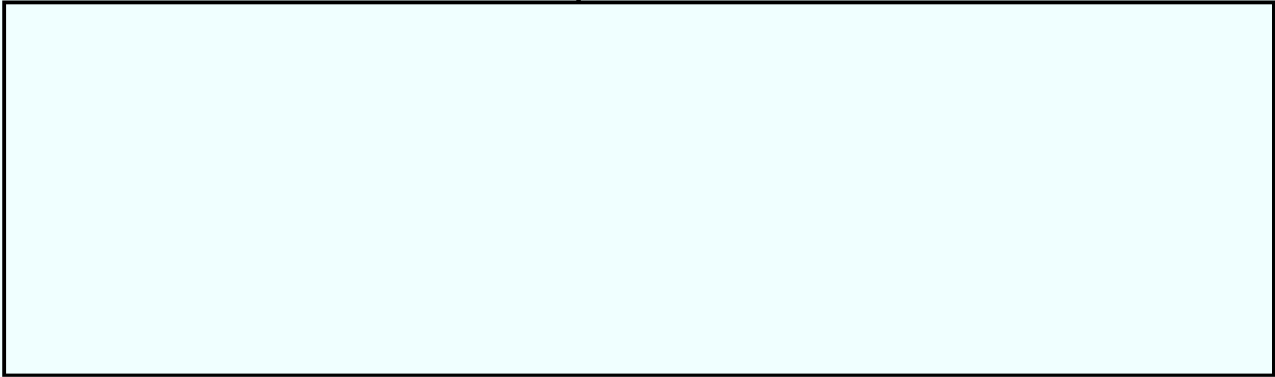


b1
b5
b7A

~~SECRET~~

~~SECRET~~

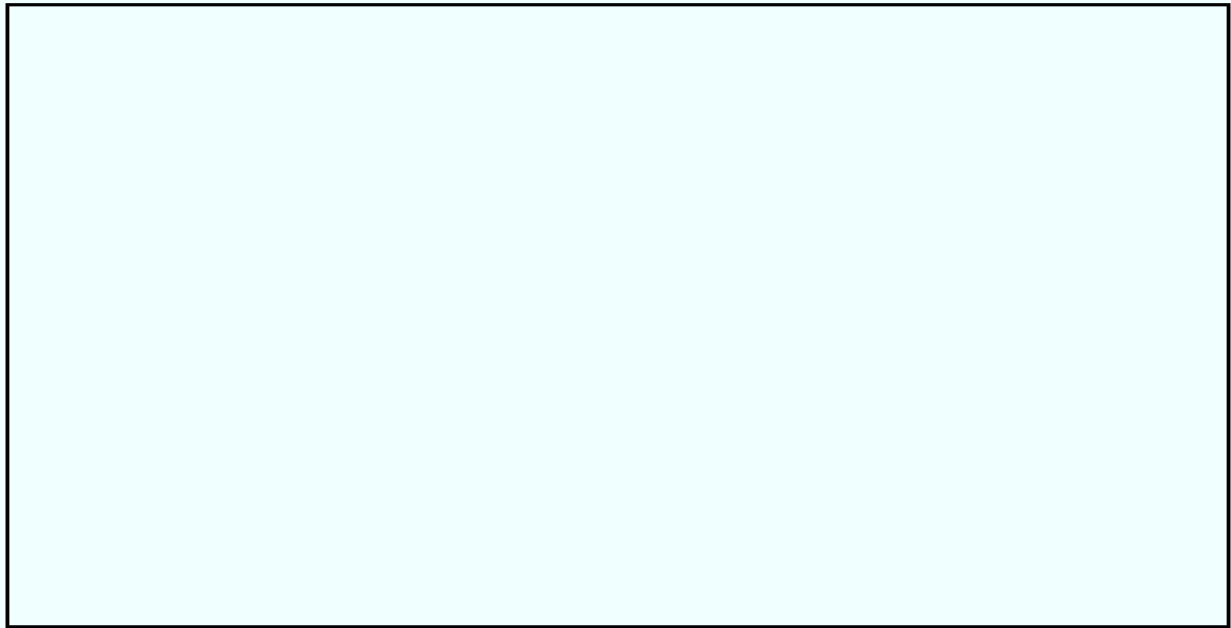
b5



b5

b6

b7C



c. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which Congress should consider?

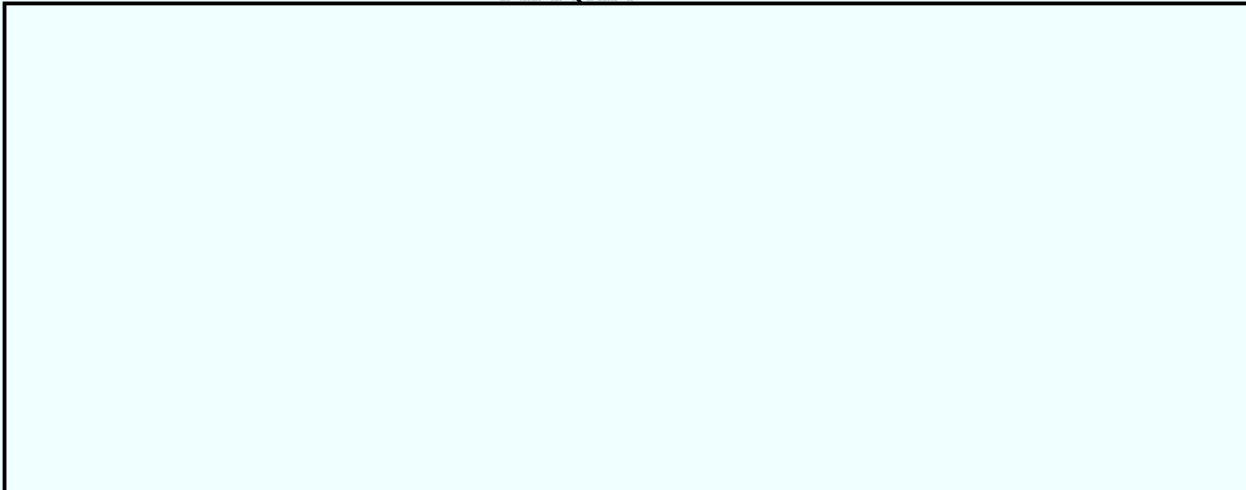
b5



101 d. OGC. According to court records, no criminal charges were ever filed against Mayfield. Instead, he was detained as a material witness. Why was Mayfield held as a material witness and not charged with any criminal conduct?

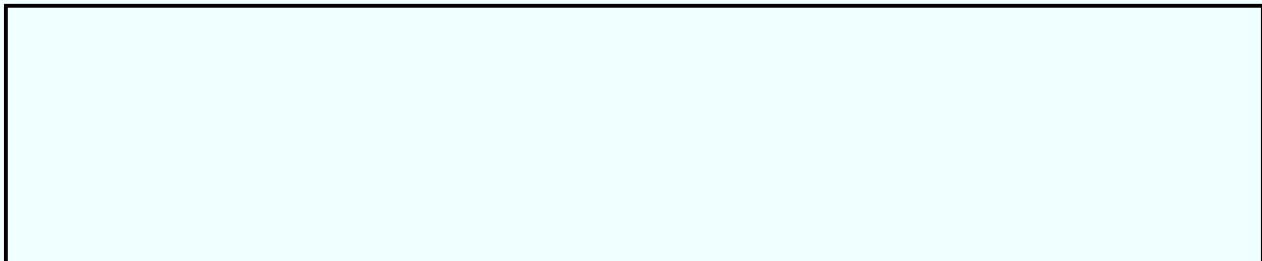
~~SECRET~~

~~SECRET~~



b6
b7C

100 e. CTD (in coordination with OGC). Mayfield has stated that he believes that his home was secretly searched before he was declared a material witness and detained. Prior to, or during his detention, was the Mayfield residence or office searched pursuant to a warrant under the Foreign Intelligence Surveillance Act (FISA) or a delayed notification search warrant? If the latter, please indicate (a) the basis for seeking delayed notice of the search warrant and (b) the time period requested and granted for delaying notice.



b1
b5
b6
b7C

(S)

103. OGC. In September 2003, the U.S. Department of Justice disclosed that it had not yet used section 215 of the USA PATRIOT Act. On March 9, 2004, I sent a letter to the Attorney General asking him to clarify whether section 215 has been used since September 18, 2003. (Copy of letter attached.)

a. Please indicate whether section 215 has been used since September 18, 2003.

b. If section 215 has been used, please describe how it has been used. How many U.S. persons and non-U.S. persons were targets of the investigation? Was the section 215 order served on a library, newsroom, or other First Amendment sensitive place? Was the product of the search used in a criminal prosecution?

b1
b2
b7E

Response: a.



(S)

~~SECRET~~

~~SECRET~~

~~(S)~~

b.

b1
b2
b7E

(S)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 26

Page 428 ~ Duplicate

Page 429 ~ Duplicate

Page 430 ~ Duplicate

Page 431 ~ Duplicate

Page 432 ~ Duplicate

Page 433 ~ Duplicate

Page 434 ~ Duplicate

Page 435 ~ Duplicate

Page 436 ~ Duplicate

Page 437 ~ Duplicate

Page 438 ~ Duplicate

Page 439 ~ Duplicate

Page 440 ~ Duplicate

Page 441 ~ Duplicate

Page 442 ~ Duplicate

Page 453 ~ Duplicate

Page 454 ~ Duplicate

Page 455 ~ Duplicate

Page 456 ~ Duplicate

Page 457 ~ Duplicate

Page 458 ~ Duplicate

Page 459 ~ Duplicate

Page 460 ~ Duplicate

Page 461 ~ Duplicate

Page 462 ~ Duplicate

Page 463 ~ Duplicate

FEDERAL BUREAU OF INVESTIGATION

Precedence: IMMEDIATE

Date: 12/11/2001

To: All Field Offices

Counterterrorism

National Security

Attn: ADIC; SAC; CDC
FCI/IT Supervisors
AD Watson; DADSs
Section Chiefs
AD Gallagher; DADs
Section Chiefs

From: General Counsel
National Security Law Unit, Room 7075

Contact:

b6

b7C

Approved Mueller Robert S III
By: Pickard Thomas J
Parkinson Larry R
Bowman M E

Drafted By:

b6

b7C

Case ID 66F-HQ-A1255972
#:

Title: NATIONAL SECURITY LETTER
MATTERS

Synopsis: Provides guidance on the preparation, approval, and service of National Security Letters (NSLs).

Reference: 66F-HQ-A1255972 Serial 15

Enclosure(s): 1) Subscriber Information NSL Model
2) Toll Billing Records NSL Model
3) Electronic Subscriber Information NSL Model
4) Electronic Communication Transactional Records NSL Model
5) Financial Records NSL Model
6) Identity of Financial Institutions NSL Model
7) Consumer Identifying Information NSL Model
8) Subscriber/Electronic Subscriber (EC) Model
9) Toll/Transactional Records EC Model
10) Financial Records EC Model
11) Financial Institutions/Consumer Identity EC Model
12) ECPA NSL Checklist
13) RFPA NSL Checklist
14) FCRA NSL Checklist

Details: In the referenced communication, dated 11/09/2001, the Director of the FBI delegated the authority to certify NSLs to the following officials: (1) the Deputy Director; (2) The Assistant Directors (ADs) and all Deputy Assistant Directors (DADs) of the Counterterrorism Division (CTD)

and the National Security Division (NSD); (3) the General Counsel and the Deputy General Counsel for National Security Affairs (DGC), Office of the General Counsel (OGC); (4) the Assistant Director in Charge (ADIC), and all Special Agents in Charge (SACs), of the New York, Washington, D.C., and Los Angeles field divisions; and (5) the SACs in all other field divisions. The purpose of this electronic communication is to provide comprehensive guidance on the preparation, approval, and service of NSLs.

1. Introduction to National Security Letters

NSLs are administrative subpoenas that can be used to obtain several types of records. There are three types of NSLs. First, pursuant to the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2709, the FBI can issue NSLs for: (1) telephone subscriber information (limited to name, address, and length of service); (2) telephone local and long distance toll billing records; and (3) electronic communication transactional records. Second, pursuant to the Right to Financial Privacy Act (RFPA), 12 U.S.C. § 3414(a)(5), the FBI can issue NSLs to obtain financial records from banks and other financial institutions. Finally, pursuant to the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681u, the FBI can issue NSLs to obtain consumer identifying information and the identity of financial institutions from credit bureaus.

NSLs are tools available in investigations conducted under the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations (FCIG). The FCIG currently provide that an NSL can be issued during the course of a full international terrorism or foreign counterintelligence investigation. **NSLs cannot be used in criminal investigations unrelated to international terrorism or clandestine intelligence activities.** Given the new statutory language, the OGC and DOJ have taken the position that NSLs also may be authorized in foreign counterintelligence (FCI) and international terrorism (IT) preliminary inquiries (PIs), with prior coordination through the relevant NSD or CTD unit at FBIHQ. This position is based on the conclusion that all investigations authorized under the FCIG, including PIs, are to "protect against international terrorism or clandestine intelligence activities," as required by the NSL statutory authorities. At present, however, issuing an NSL in the context of a PI will require a waiver or modification of the FCIG. Obtaining such a waiver currently is possible only in international terrorism cases. The FCIG are being revised, but this revision may take some time. Thus, whenever the information sought is relevant to an established full investigation, the field likely will find it more efficient to issue an NSL out of the related full investigation than to request one in a PI.

2. General Policy on the Use of NSL Authority

NSLs are powerful investigative tools, in that they can compel the production of substantial amounts of relevant information. However, they must be used judiciously. The USA PATRIOT Act greatly broadened the FBI's authority to gather this information. However, the provisions of the Act relating to NSLs are subject to a "sunset" provision that calls for the expiration of those provisions in four years. In deciding whether or not to re-authorize the broadened authority, Congress certainly will examine the manner in which the FBI exercised it. Executive Order 12333 and the FCIG require that the FBI accomplish its investigations through the "least intrusive" means. Supervisors should keep this in mind when deciding whether or not a particular use of NSL authority is appropriate. The greater availability of NSLs does not mean that they should be used in every case.

In addition, the removal of any requirement for FBIHQ coordination in the issuing of NSLs creates the possibility of duplicate requests for the same information by different field offices. Field offices must take steps to avoid this. In particular, the field should check FBI databases (ACS, Telephone Application, etc.) and open sources to see if the information sought has already been obtained by the FBI or whether it is publically available. This is particularly important when considering issuing NSLs for telephone or electronic communications data under the Electronic

Communications Privacy Act (ECPA). Unlike the criminal authorities in ECPA, the NSL authority does not require the government to reimburse carriers or Internet Service Providers (ISPs) for the cost of producing the requested information. A dramatic increase in duplicate NSLs will only augment existing pressure to require governmental reimbursement.

Individual field offices have the responsibility for establishing and enforcing an appropriate review and approval process for the use of NSL authorities.

3. The Mechanics of Producing NSLs

For all types of NSLs, the issuing office needs to prepare two documents: (1) the NSL itself; and (2) an EC approving the NSL and documenting the predication. Model NSLs and ECs for all variations of the three types of NSLs are included as attachments to this communication. These materials will also be placed on the NSLU Intranet Website and will be distributed by GroupWise e-mail. Once the initial implementation of these new authorities is accomplished, NSLU will work to develop a macro or form to further streamline the NSL process.

A. The NSL

There are presently seven variations of the three NSL types: 1) subscriber information; 2) toll billing records; 3) electronic subscriber information; 4) electronic communication transactional records; 5) financial records; 6) identity of financial institutions; and 7) consumer identifying information. This section will discuss the features that these variations share in common and highlight the differences.

All NSLs must be addressed to an appropriate company point of contact. NSLU will place a list of known points of contact on its intranet website. However, the responsibility for ensuring that the company point of contact is up to date belongs to the drafting field division. Field divisions should advise NSLU of any new points of contact, or when a particular point of contact is no longer valid. Please note that the company point of contact address does not include a zip code, because NSLs must be hand-delivered.

The first paragraph of every NSL provides the appropriate statutory authority for the request, identifies the types of records requested, and provides available identifying information so that the company can process the NSL request. It is this first paragraph that contains the differences that warrant the seven NSL varieties.

Subscriber and electronic subscriber NSLs should have a specific date for each of the phone numbers/e-mail addresses requested. Typically, the specific date is going to be the date that the phone number or e-mail address was used in communication with the subject of the investigation. Any phone numbers identified in a subscriber request should contain all ten digits of the phone number, including the area code.

Toll billing record and electronic communication transactional record requests should have a range of dates for each of the phone numbers/e-mail addresses requested. The date range may be from inception to present, or some other specified date range relevant to the investigation. Any phone numbers identified in a toll billing record request should contain all ten digits of the phone number, including the area code.

Financial record requests should include all available identifying information to facilitate the financial institution's records search. Typically, such identifying information includes: name, account numbers, social security number, and date of birth. The time period for financial record requests is typically from inception of account(s) to present, although a more specific date range may be used.

Credit record requests are similar to financial requests in that they should include available identifying information to facilitate the credit agency's records search. Typically, such identifying information includes: name, social security number, and date of birth. There is no need to specify a date range for credit record requests because these requests seek all records where the consumer maintains or has maintained an account.

The second paragraph of every NSL contains the statutorily required certification language. The certification language is virtually identical for every NSL. However, please note that the certification language used in the financial records NSLs is slightly different than the others in that it states "the records are sought for foreign counterintelligence purposes" Financial records also contain an additional certification that the FBI has complied with all applicable provisions of the RFPA. Use of the model NSLs will ensure that the proper certifications are made.

The next paragraph contains an admonition for the phone company, ISP, financial institution, or credit agency receiving the NSL. The paragraph warns that no officer, employee, or agent of the company may disclose that the FBI has sought or obtained access to the requested information or records.

The last substantive paragraph instructs the company point of contact to provide the records personally to a representative of the delivering field division. It also states that any questions should be directed to the delivering field division. This last paragraph requires the person preparing the NSL to input the appropriate delivering field division in two places.

The model NSLs for financial records and electronic communication transactional records each have a separate attachment. These attachments provide examples of information which the company might consider to be financial or electronic communication transactional records.

Finally, the NSL is an unclassified document because it does not detail the specific relevance of the requested records to an authorized FBI investigation. There is no need to classify the NSL when attaching it to the cover EC.

B. The Cover EC

The Cover EC serves four essential functions in the NSL process: (1) it documents the predication for the NSL by recording why the information sought is relevant to an investigation; (2) it documents the approval of the NSL by relevant supervisors and the legal review of the document; (3) it contains the information needed to fulfill the Congressional reporting requirements for each type of NSL; and (4) it transmits the NSL to the requesting squad or delivering field division for delivery to the appropriate telecommunications carrier, ISP, financial institution, or credit agency. There are four varieties of model ECs provided with this communication: (1) subscriber/electronic subscriber information; (2) toll billing/electronic communication transactional records; (3) financial records; and (4) credit information. When preparing an NSL request, the field should use one of these model ECs, giving special consideration to the elements discussed in this section.

1) Field Descriptors

This section will generally explain how most of the EC field descriptors should be completed. The "**Precedence**" descriptor will typically be "ROUTINE." The "**Date**" descriptor should reflect the date the NSL and the EC were approved. The "**To**" descriptor will always include "General Counsel" and the requesting squad's field division. It may also include the name of the delivering field division (always Los Angeles in the case of FCRA NSLs) and the office of origin, if applicable. The "**Attn**" descriptor should include the name of the Chief, NSLU, and the squad supervisors and case agents from the requesting squad, delivering field division, and office

of origin, if applicable and if known. The credit model EC identifies the FBI personnel working on Squad 4, Santa Ana RA, who are currently responsible for the service of FCRA NSLs. The "From" descriptor should identify the certifying official's field division, and include the title of the certifying official. The "Contact" descriptor should reflect the name and phone number of the requesting squad case agent. The "Drafted By" descriptor should reflect the name of the person who prepared the NSL package. The "Case ID #" descriptor must contain the case file number relevant to the request, and the case file numbers indicated in the model EC. The "Title" descriptor should list the subject's name, any known aliases, whether the investigation is an FCI or IT investigation directed at a particular foreign power, and identify the office of origin, e.g., WILLIAM BADGUY, AKA BILL BADGUY, FCI-IRAQ, OO: NEW YORK. The "Synopsis" descriptor should use the standard boilerplate contained in the appropriate model EC. The "Derived From" descriptor should be "G-3" in bold typeface. The "Declassify On" descriptor should be "X1" in bold typeface. the "Full Investigation Instituted" descriptor should contain the date the full FCI or IT investigation was opened on the subject and indicate whether the subject is a U.S. person. Please note that the word "Field" has been deleted from the field descriptor contained in the standard EC macro. In the unlikely event that an NSL is issued during a PI with prior FBIHQ approval, the field descriptor should be edited to state "Preliminary Inquiry Instituted." The remaining descriptors can be filled in according to the model EC being used.

2) Predication and Relevance

The USA PATRIOT Act has greatly simplified the NSL process. The FBI official authorizing the issuance of an NSL is no longer required to certify that there are specific and articulable facts giving reason to believe that the information sought pertains to a foreign power, or an agent of a foreign power. NSLs may now be issued upon a certification of relevance to an authorized investigation to protect against international terrorism or clandestine intelligence activities.

Accordingly, the first paragraph in the "Details" section of the EC should contain the predication for the full investigation and identify the relevance of the requested records to the investigation. Both the predication and relevance should be stated clearly and concisely. The predication should track with the predicates contained in FCIG, Section III.C.1. For example, the predication might state, "A full foreign counterintelligence investigation of subject, a Non-U.S. person, was authorized in accordance with the Attorney General Guidelines because he may be a suspected intelligence officer for the Government of Iraq." Another example might state, "A full international terrorism investigation of subject, a U.S. person, was authorized in accordance with the Attorney General Guidelines because he may be engaged in international terrorism activities by raising funds for HAMAS."

The relevance requirement ties the requested records to the appropriate full investigation. For example, relevance could be established by stating, "This subscriber information is being requested to determine the individuals or entities that the subject has been in contact with during the past six months." Another example might state, "The subject's financial records are being requested to determine his involvement in possible HAMAS fund raising activities."

3) Approval

The second paragraph in the "Details" section and the "Approved By" descriptor field of the EC should reflect the level of the official approving the issuance of the EC and signing the NSL's certification. Prior to certification, every NSL and cover EC issued by the field division should be reviewed by the squad supervisor, the Office of the Chief Division Counsel, and the ASAC. Lawyers reviewing NSL packages should use the checklists provided with this communication to ensure legal sufficiency. The last step in the approval process occurs when the certifying official (Deputy Director, ADs, General Counsel, ADICs, DADs, DGC, or SACs) personally signs the NSL and initials the EC. Certifying officials may not further delegate signature authority.

4) Reporting Requirements

NSLU will continue to prepare the mandatory reports to Congress required for each NSL type. To ensure that NSLU receives sufficient information to prepare these reports, it is critical that the person preparing the NSL package follow the NSL and EC models very carefully. The second lead in every model EC requests NSLU to "record the appropriate information needed to fulfill the Congressional reporting requirements for NSLs." NSLU will be able to compile the reporting data provided that the cover EC includes the case file number, the subject's U.S. person status, the type of NSL issued, and the number of phone numbers, e-mail addresses, account numbers, or individual records being requested in the NSL. Once NSLU has entered this reporting data into its NSL database, it will clear the lead set in the cover EC.

5) Transmittal

Often, the squad requesting the NSL will be able to hand-carry the NSL locally to the appropriate company point of contact. However, in many situations, the field division drafting the NSL will have to get it delivered by another field division. In these situations, the drafting division should attempt to identify the squad and personnel at the delivering field division who will be responsible for delivering the NSL. In the event that the office of origin is different than either the drafting division or delivering division, the person drafting the NSL package should ensure that the case agent from the office of origin receives a copy of the package. The first lead in the model ECs should direct the requesting squad or delivering field division to deliver the attached NSL. If the delivering division is different than the drafting division or the office of origin, then this first lead should also request the delivering division to submit the results to the drafting division and/or the office of origin.

4. NSL Preparation Assistance

Some field divisions may, for a variety of reasons, opt not to exercise their delegated authority to issue NSLs. Other field divisions may exceed their capacity to issue NSLs and seek assistance in handling the overflow. NSLU will continue to process any NSL request that it receives. Field divisions should send their requests directly to NSLU, with information copies to the FBIHQ substantive unit. Such requests must contain all the information identified in this communication as necessary to prepare the NSL package. NSLU anticipates that it will be able to process such requests within one to three business days.

Any questions regarding this communication may be directed to [redacted]
[redacted] NSLU, OGC, at [redacted]

b6

b7c

LEAD(s):

Set Lead 1: (Adm)

ALL RECEIVING OFFICES

Distribute to all supervisory personnel involved in the National Security Letter process.

SECRET

b5

DATE: 12-08-2005
CLASSIFIED BY 65179dmh/baw
REASON: 1.4 (c 05-cv-0845)
DECLASSIFY ON: 12-08-2030

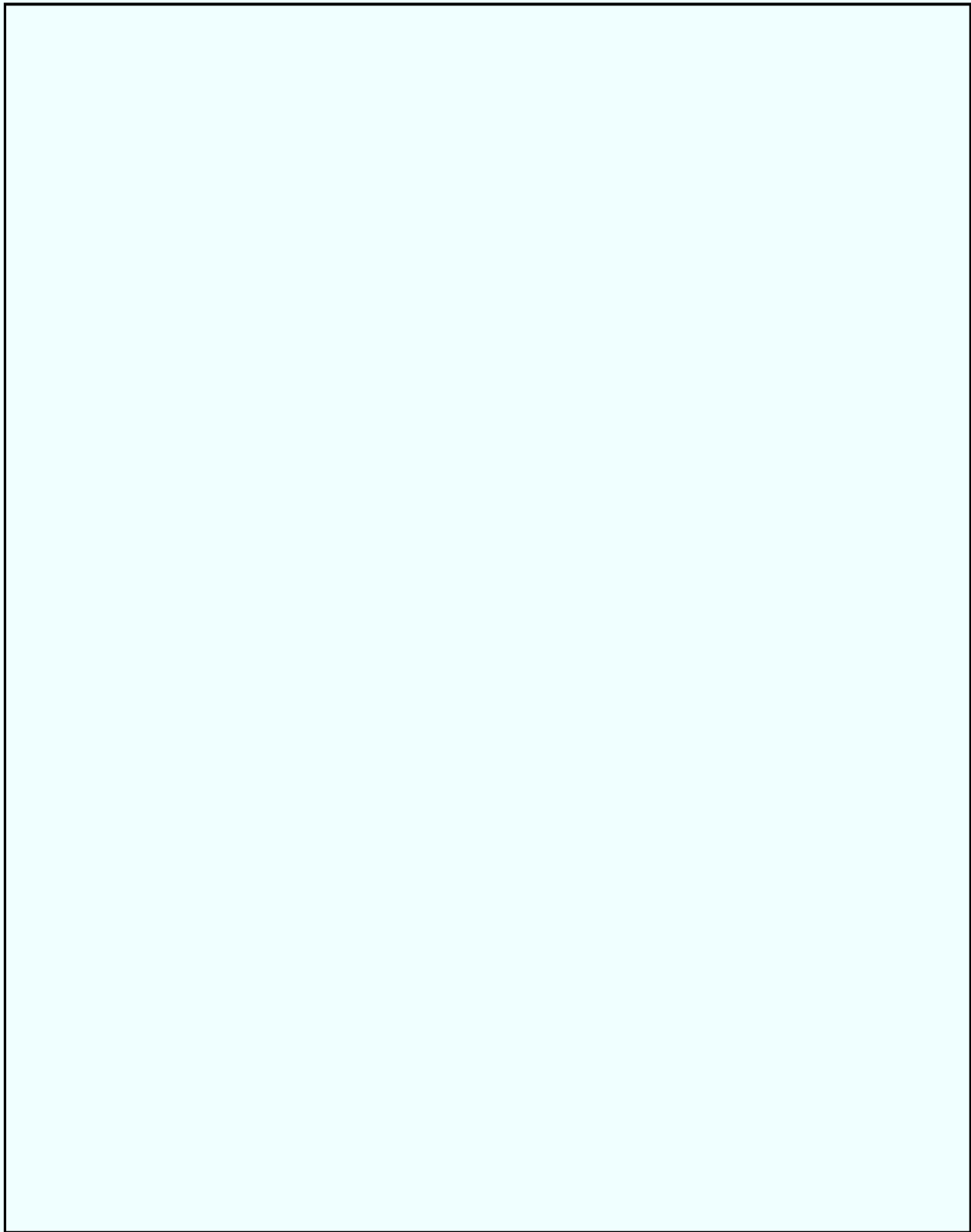
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

SECRET

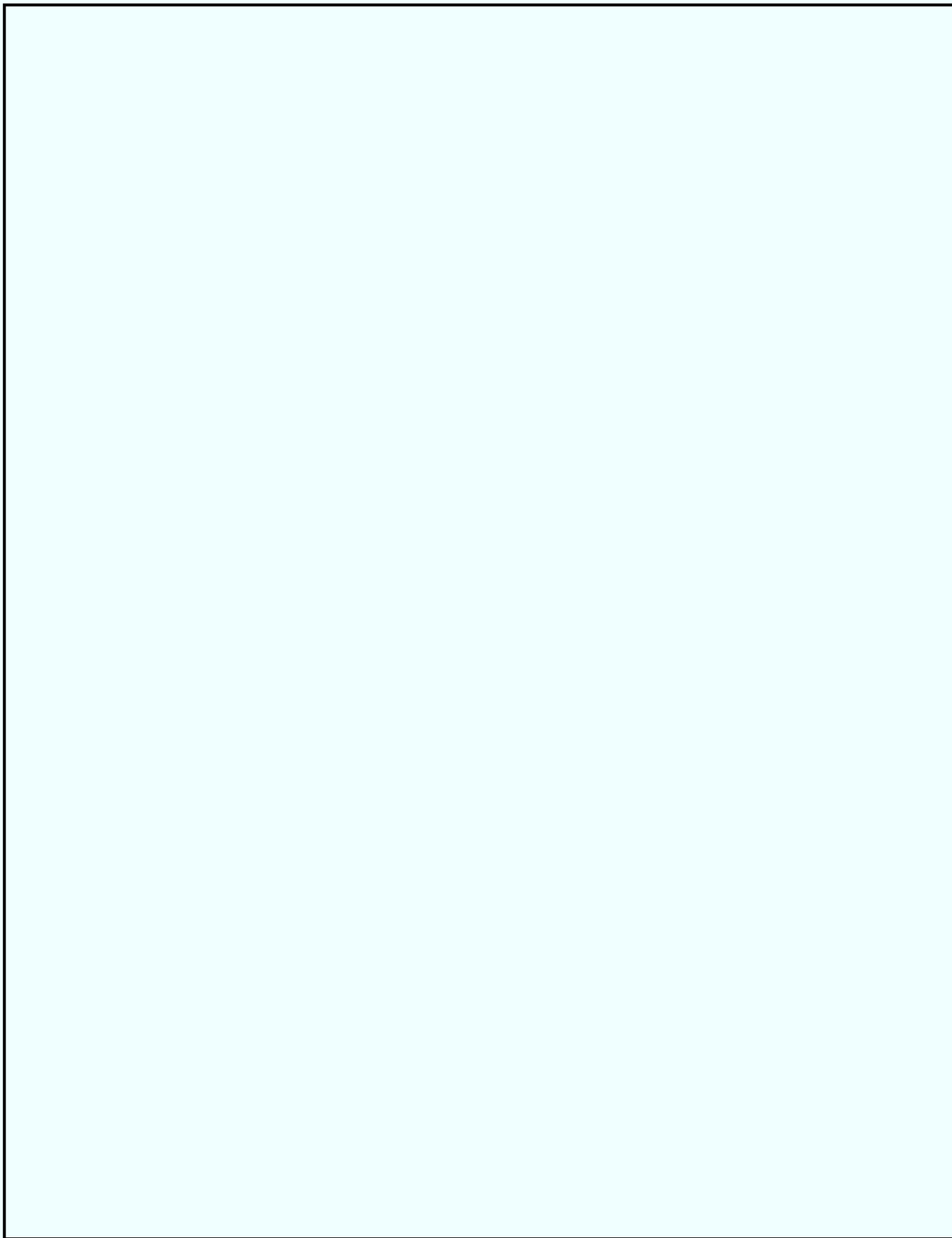
b5

b6

b7C



SECRET



b5

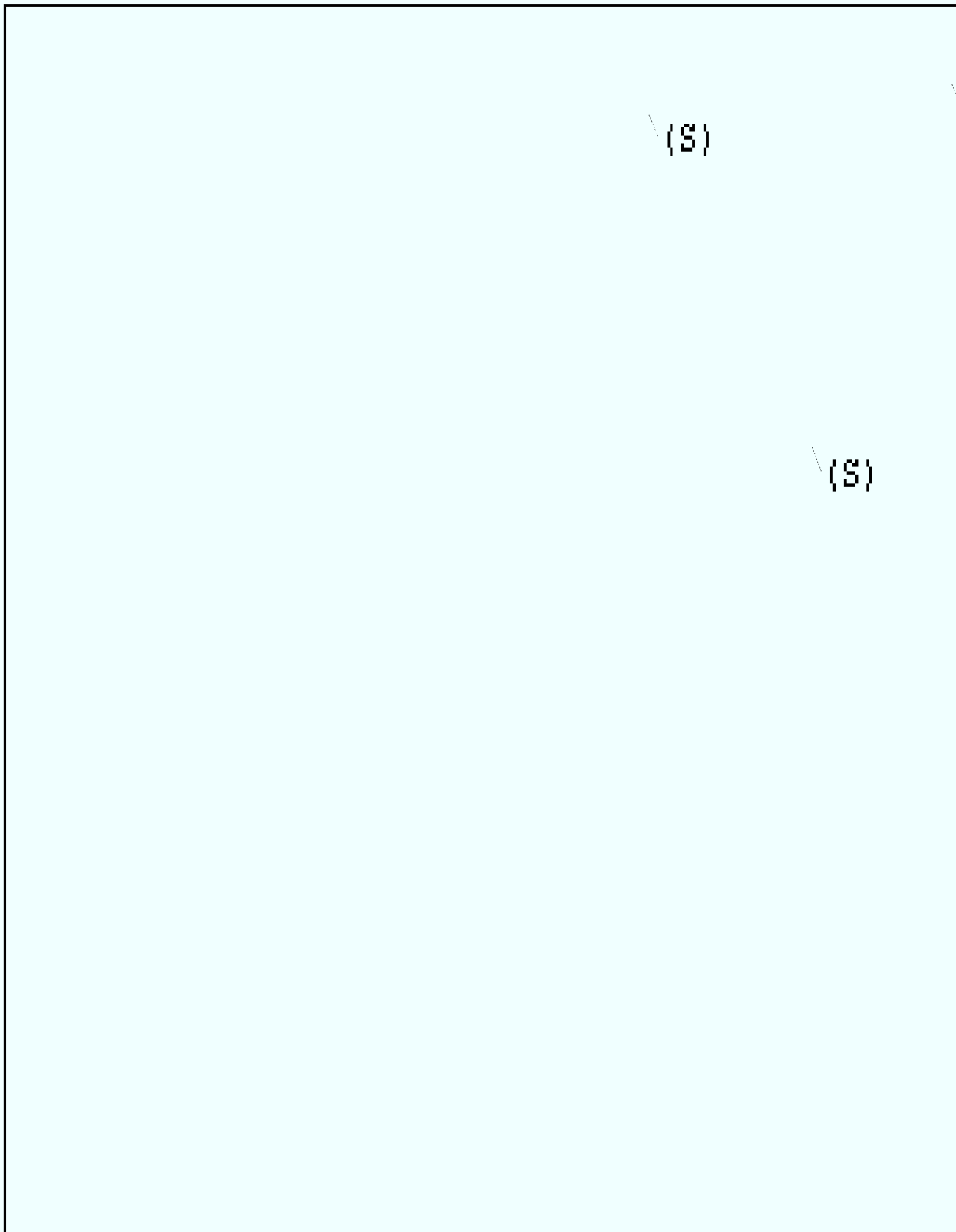
b2

b7D

b6

b7C

b7A



(S)

(S)

(S)

(S)

(S)

b5
b2
b7C
b1

SECRET

(S)

b5
b2
b7E
b1

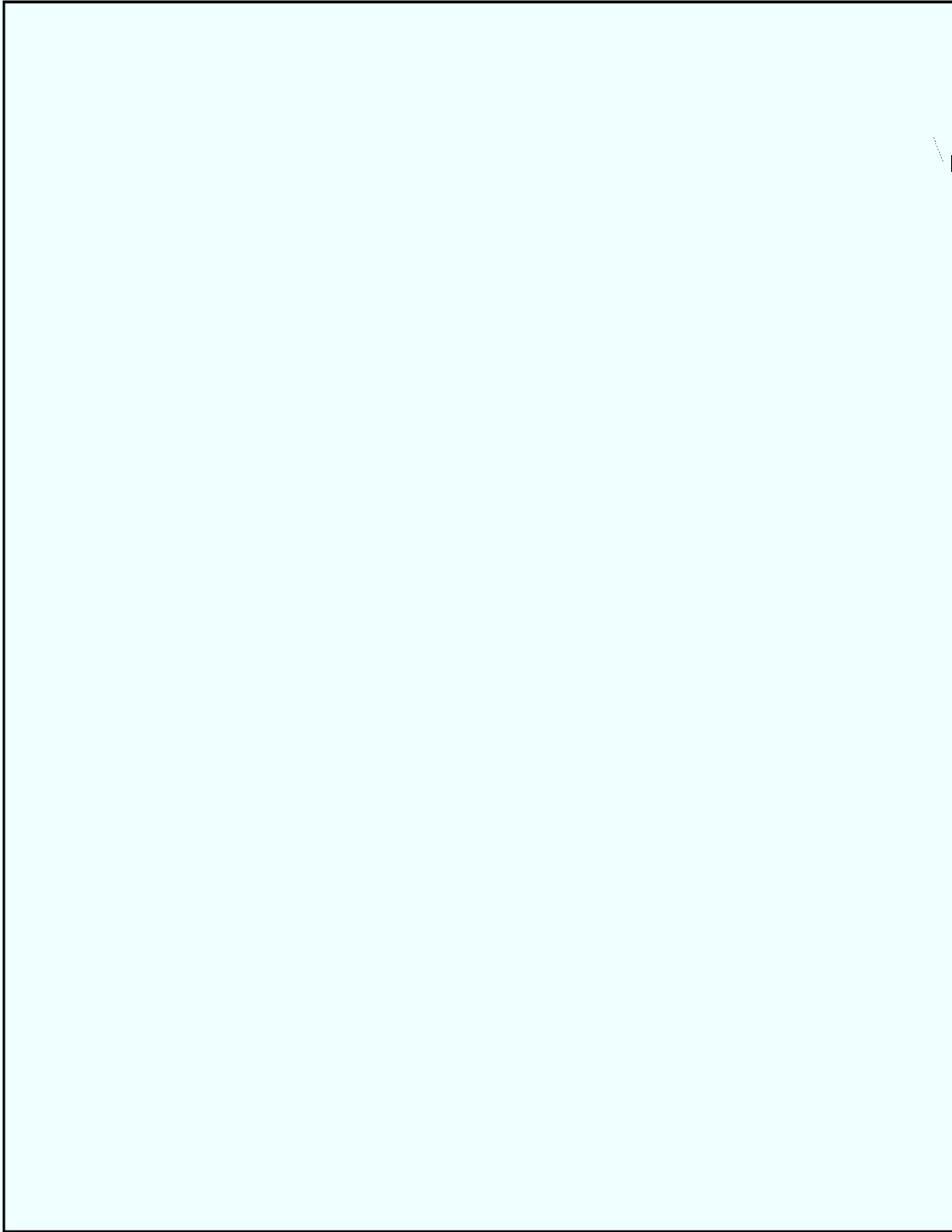
SECRET



b5
b2
b7E
b1

(S)

SECRET



(S)

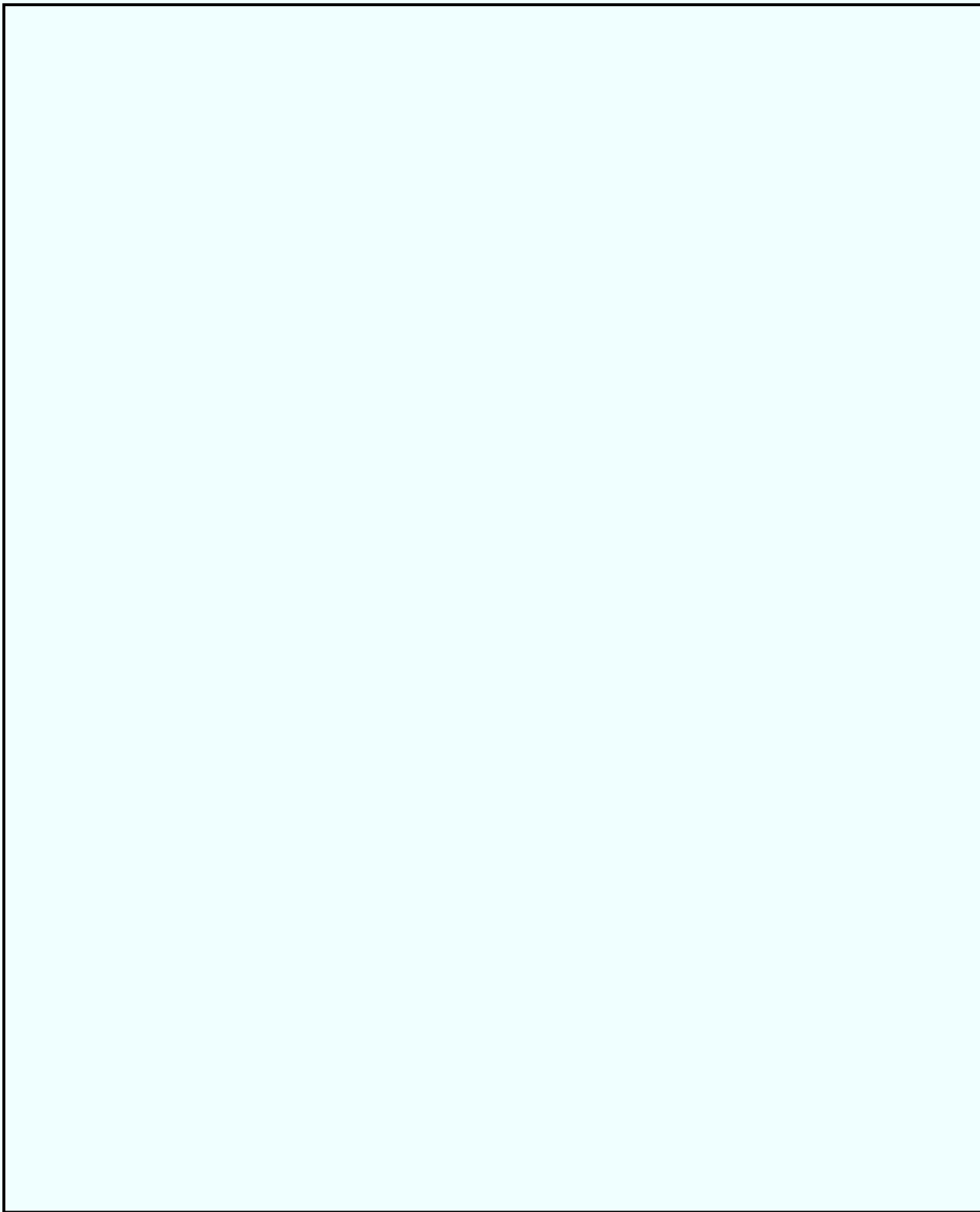
b5
b2
b7E
b1

(S)

SECRET

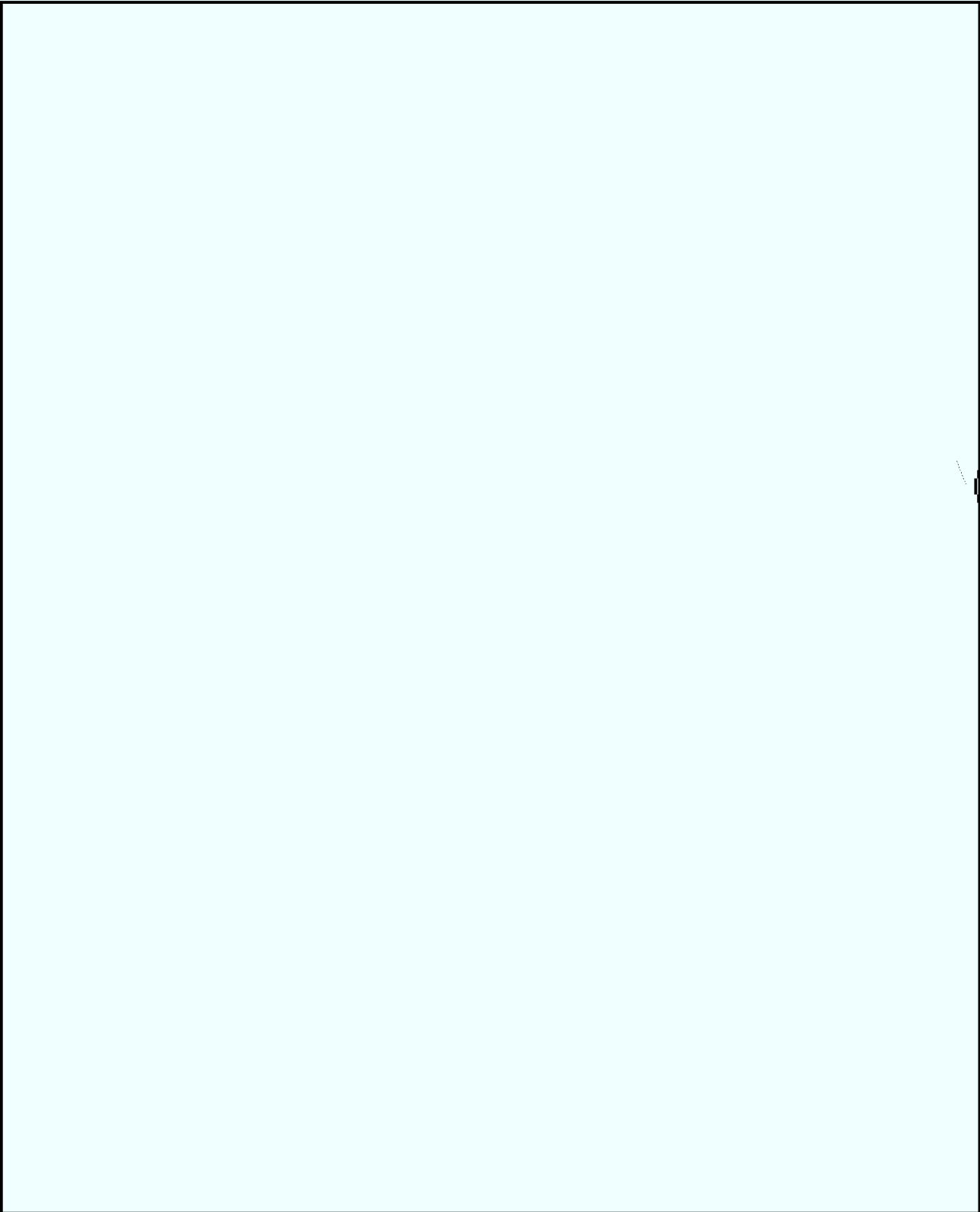
b5
b2
b7E
b6
b7C

SECRET



b5
b7A
b2
b7E

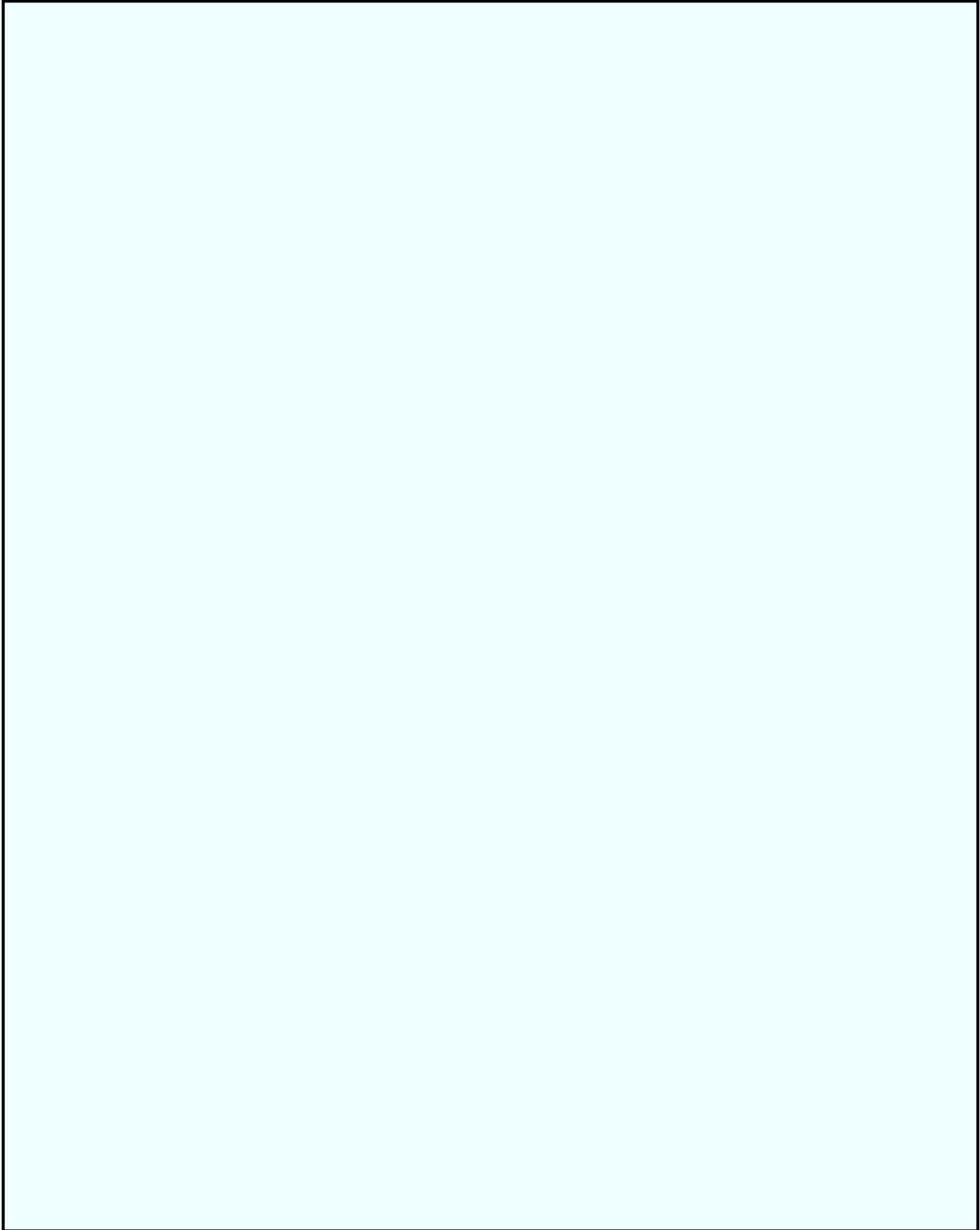
SECRET



(S)

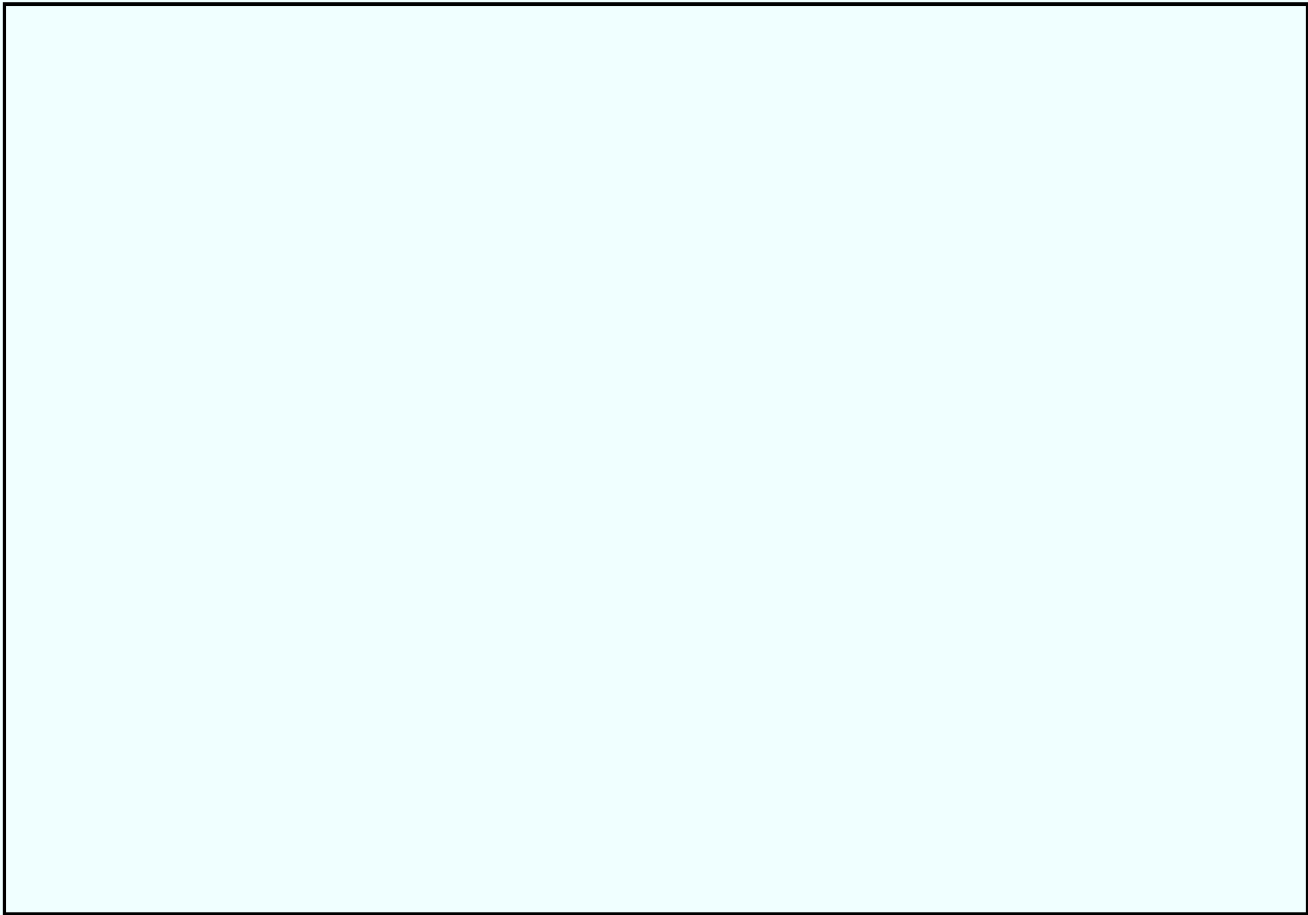
b5
b2
b7E
b1

SECRET



b5
b2
b7E
b7A

SECRET



b5
b2
b7E

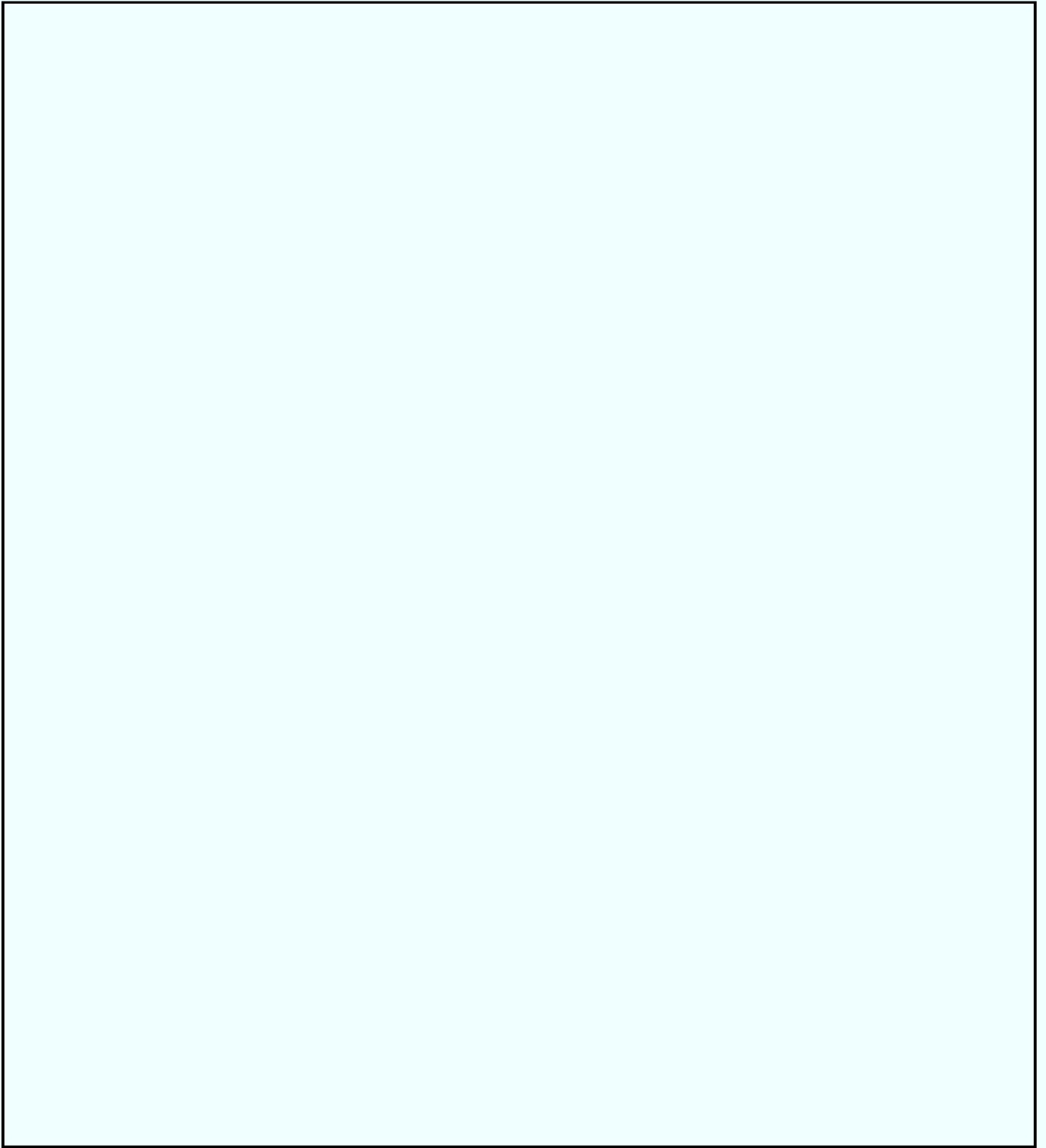
SECRET

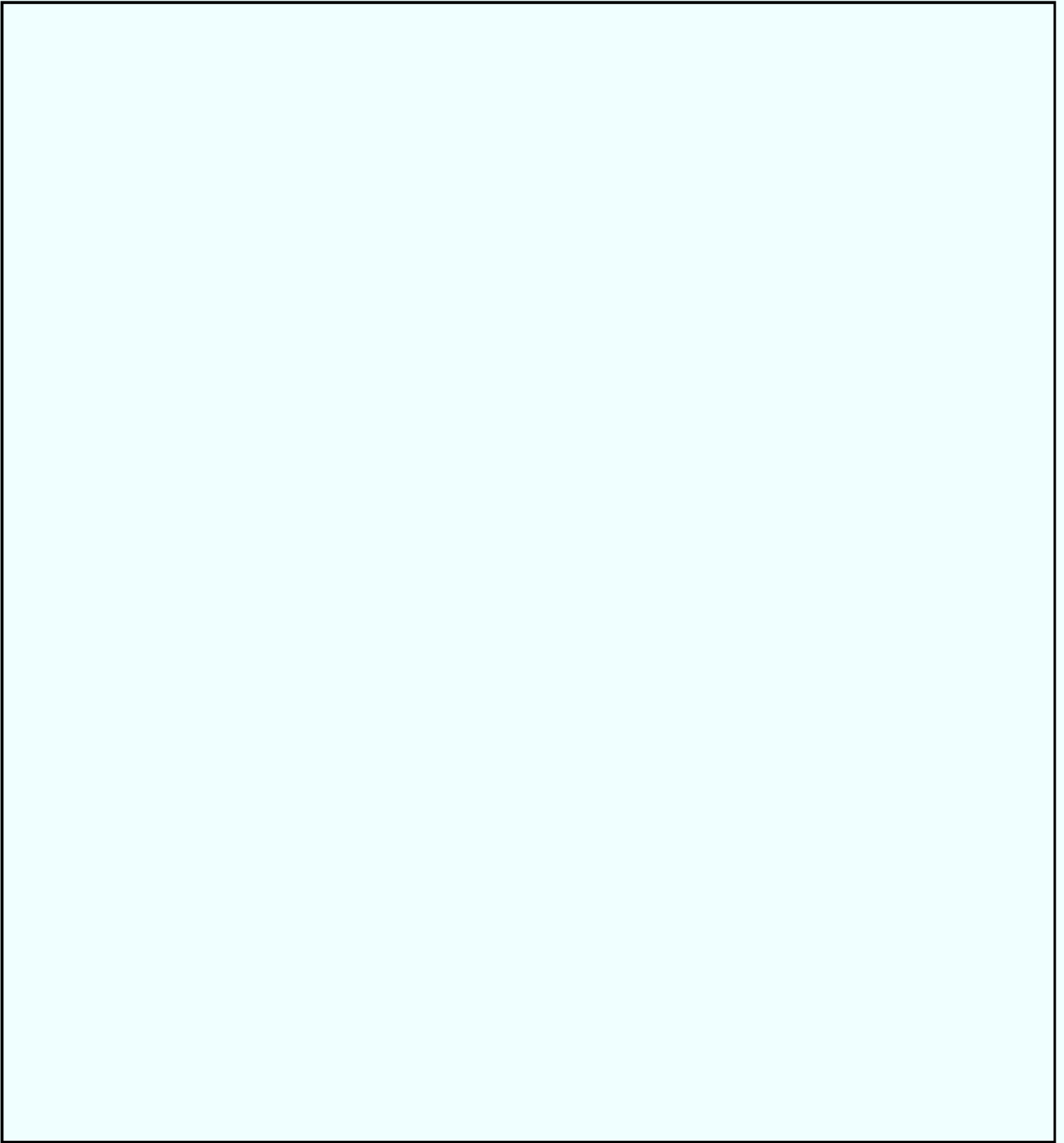
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-01-2005 BY 65179 DMH / JHF 05-CV-0845

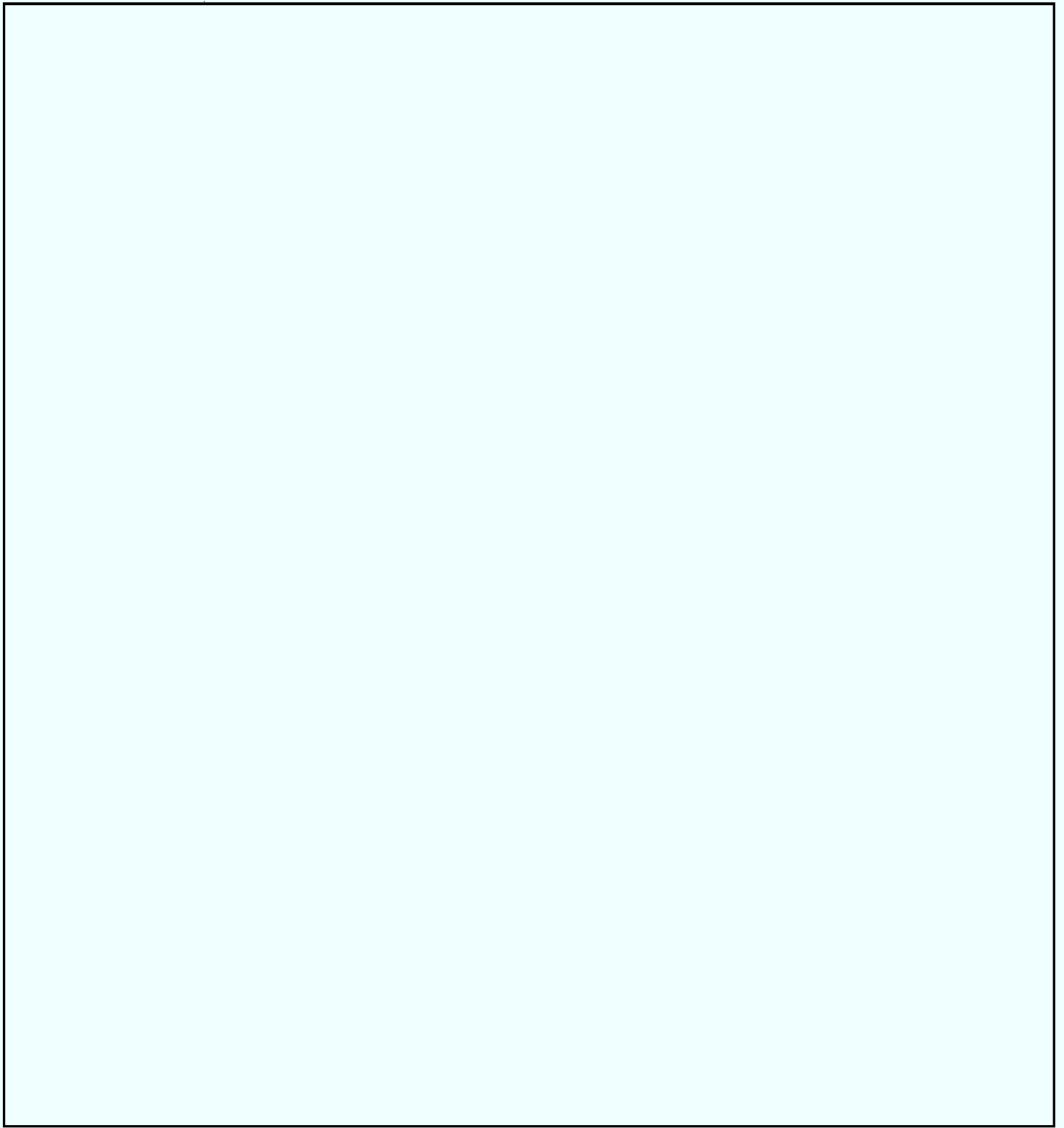
b5

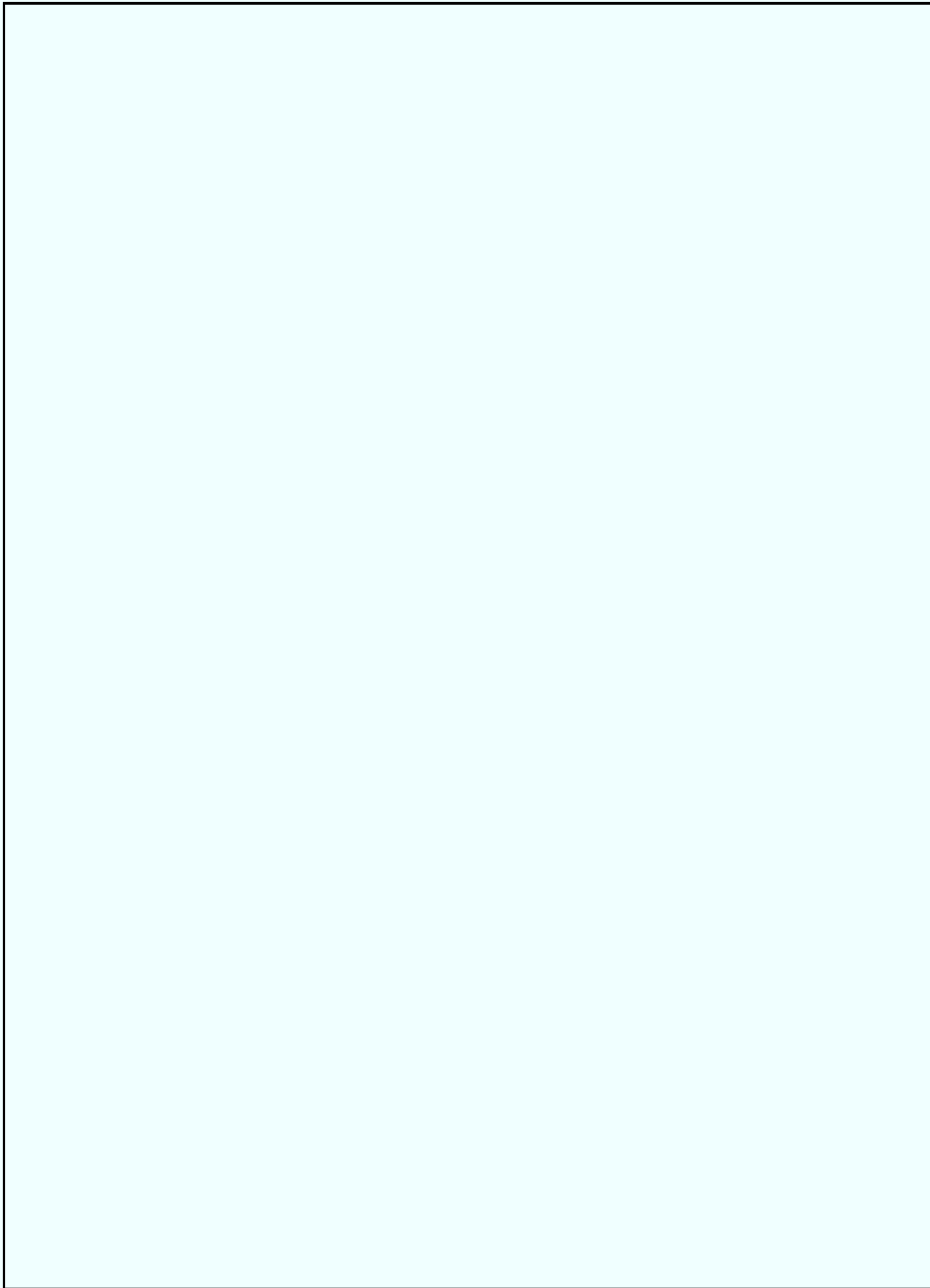
b5

1









b5

b5


REVISED 3/22/05

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-01-2005 BY 65179 DMH /JHF 05-CV-0845

FBI
Office of General Counsel
National Security Law Branch

March 22, 2005

The Office of General Counsel has prepared this draft testimony at the request of the Office of Congressional Affairs. This request was received by the author of the draft on March 16, 2005 and the author was required to complete this draft on March 21, 2005. The Office of General Counsel does not have access to the full library of testimony given on this subject and must rely on the Office of Congressional Affairs to ensure that all testimony is consistent with prior testimony given by the Director and other senior FBI officials. The Office of General Counsel has requested that the Counterterrorism Division's International Terrorism Operations Sections I & II provide specific examples for use in this testimony. Such examples have not yet been received by the Office of General Counsel. The author of this draft testimony has therefore relied upon the examples from prior FBI testimony and DOJ reports to Congress.



REVISED 3/22/05

**Testimony of Robert S. Mueller, III
Director, Federal Bureau of Investigation
Before the United States Senate
Committee on the Judiciary**

April 5, 2005

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-01-2005 BY 65179 DMH /JHK 05-CV-0845

Good morning Mr. Chairman, Senator Leahy, and Members of the Committee. I
am pleased to be here today



b5



b5

The information sharing provisions are overwhelmingly heralded by our field offices as the most important provisions in the Patriot Act. The new ability to share crucial information has significantly altered the entire manner in which terrorism investigations are conducted, allowing for a much more coordinated and effective approach than prior to the Patriot Act.

REVISED 3/22/05

Specifically, the field offices noted that these provisions enable case agents to involve other agencies in investigations resulting in a style of teamwork that enables more effective and responsive investigations; improves the utilization of resources allowing a better focus on the case; allows for follow-up investigations by other agencies when the criminal subject leaves the U.S.; and helps prevent the compromise of foreign intelligence investigations.

Even though the law prior to the Patriot Act provided for some exchange of information, the law was complex and as a result, agents often erred on the side of caution and refrained from sharing the information. The information sharing abilities, due in part to Section 203 of the PATRIOT Act, eliminated that hesitation and allowed agents to work more openly with other government entities resulting in a much stronger team approach. Such an approach is necessary in order to prevent and detect the complex web of terrorist activity. As a result, the field offices report enhanced FBI liaison with State, Local and other Federal agencies, resulting in better relationships. [REDACTED]

[REDACTED] Even our Legal Attaches (LEGATS) notice improved relationships with foreign intelligence services. If even a portion of the information sharing capabilities are allowed to "sunset" or terminate, then the element of uncertainty that existed in the past would be re-introduced and agents [REDACTED] will again hesitate and take precious extra time to seek clarification of the information sharing restrictions prior to sharing information. This hesitation will lead to less teamwork and decreased efficiency.

b5

[REDACTED] In the aftermath of the September 11th attacks, a reliable intelligence asset identified a naturalized U.S. citizen [REDACTED] as a leader among a group of Islamic extremists residing in the U.S. The subject's extremist views, affiliations with other terrorism subjects, and his heavy involvement in the stock market increased the potential that he was a possible financier and material supporter of terrorist activities. Early in the criminal investigation it was confirmed that the subject had developed a complex scheme to defraud multiple brokerage firms of large amounts of money. The subject was arrested and pled guilty to wire fraud. The close interaction between the criminal and intelligence case investigators was critical to the successful arrest of the subject before he left the country and the eventual outcome of the case.

b5

REVISED 3/22/05

b5

Example: In one terrorism case, the only phone that the field office could show was being used by the subject was his associate's phone, and such usage was infrequent. Additionally, the field office did not have sufficient information that this associate was an

REVISED 3/22/05

agent of a foreign power. Thus, under the previous standard for a FISA pen/trap, the field office may not have succeeded in obtaining the FISA pen/trap order. The new standard established by Section 214 allowed the agents to obtain the pen/trap order by demonstrating that the information to be collected was relevant to an ongoing terrorism investigation. The information obtained by the pen/trap was valuable because it demonstrated the extent to which the subject and his associate were communicating with subjects of other terrorism investigations.

Interception of Computer Trespasser Communications under Section 217

The wiretap statute was amended explicitly to provide victims of computer attacks the ability to invite law enforcement into a protected computer to monitor the computer trespasser's communications. In the past, the law was ambiguous on this point and left open the possibility that a victim of computer hacking could not ask law enforcement to monitor the victim's own computer in an effort to prosecute and stop the intruder. The PATRIOT Act established specific requirements and limitations that must be met before the use of this provision.

b5

[REDACTED] The FBI was able to monitor the communications of an international group of "carders" (individuals who use and trade stolen credit card information). The group used chat rooms and fraudulent websites, but concealed their activities by using false identities to obtain e-mail accounts. [REDACTED]

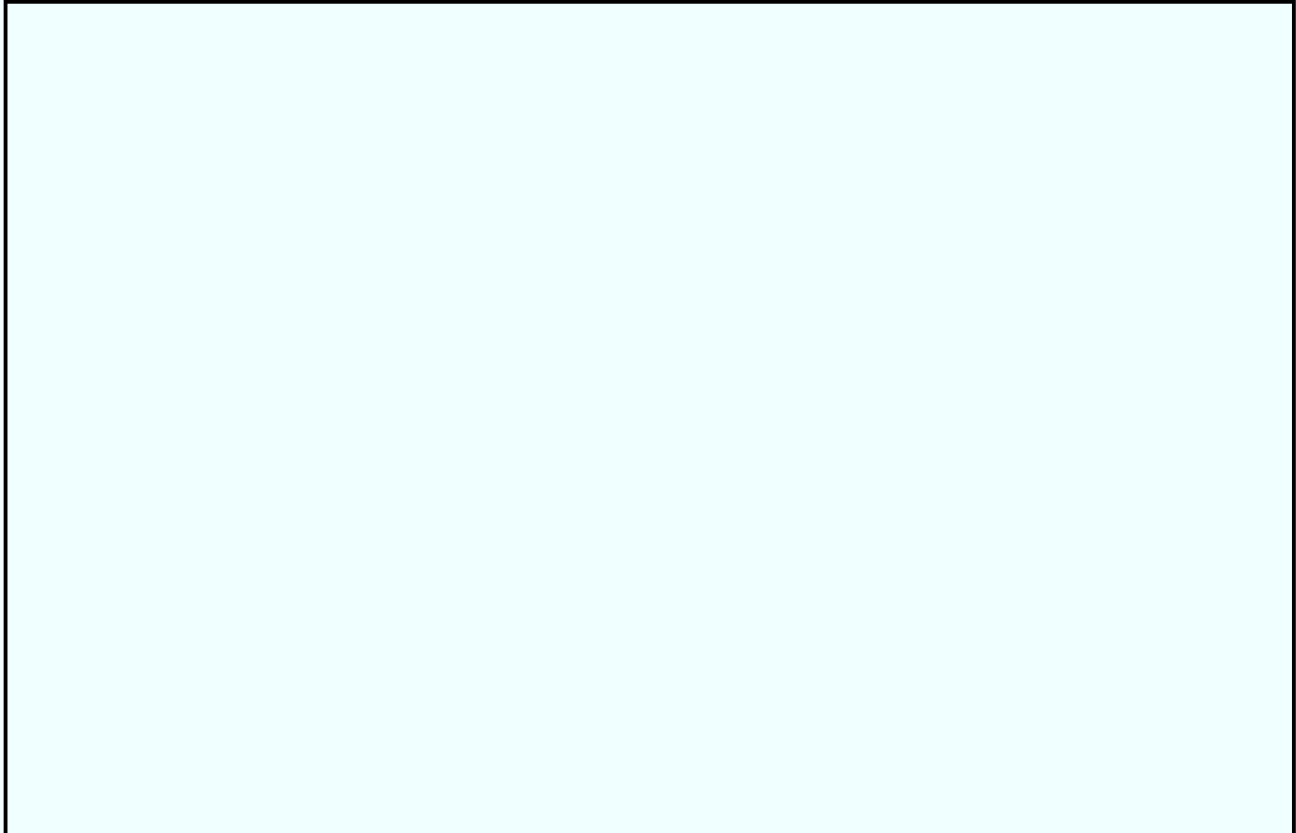
[REDACTED] The owner of the hacked computer [REDACTED] was not aware of its use as a conduit for illegal activity. When the victim noticed the unusual activity, he reported the proxy server users to the FBI as trespassers. [REDACTED]

[REDACTED] The monitoring provided leads that resulted in the discovery of the true identity of the subject. The subject was indicted in September of 2003. Without the ability to monitor these communications, it would have been unlikely that the FBI could have identified the trespassers.

Change in the "Primary Purpose" Standard of FISA under Section 218

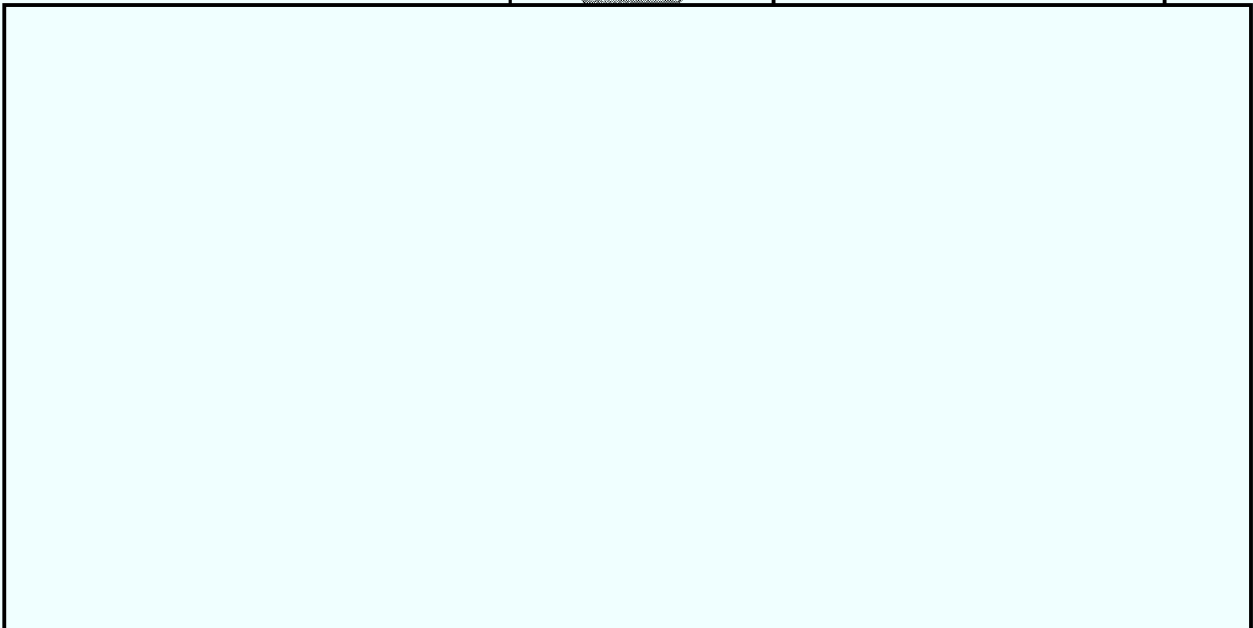
Section 218 changed FISA to require a certification that foreign intelligence be "a significant purpose" of the authority sought. Moreover, Section 504 amended FISA to allow personnel involved in a FISA to consult with law enforcement officials in order to coordinate efforts to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities, and that such consultation does not, in itself, undermine the required certification of "significant purpose." These changes were significant in eliminating "the wall" between criminal and intelligence investigations.

REVISED 3/22/05



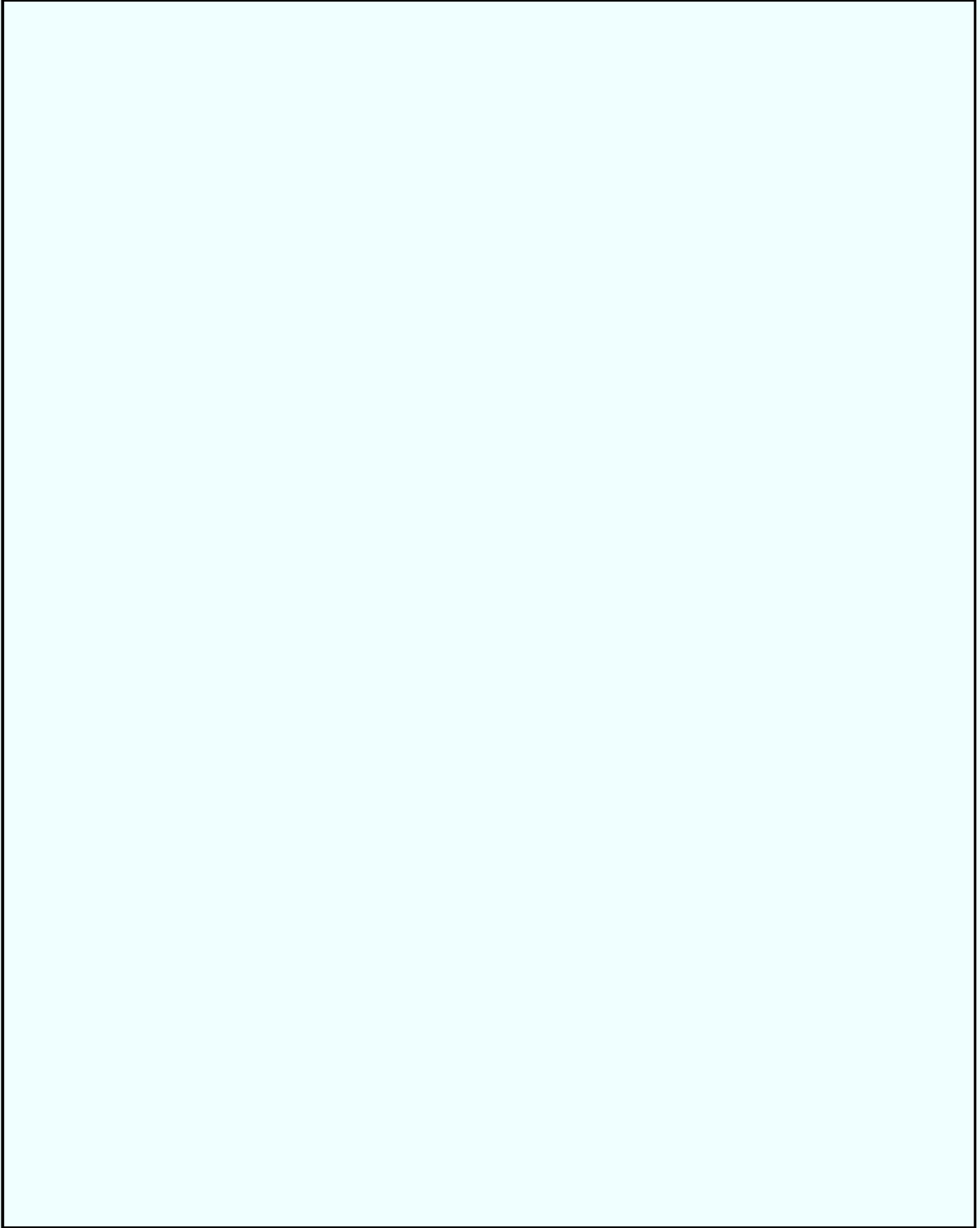
b5

Section 220 of the PATRIOT Act enabled courts to issue a search warrant with nationwide jurisdiction to compel the production of information held by a service provider, such as unopened e-mail. Previously, such a search warrant had to be issued by a court in each district where a service provider was located.



b5

REVISED 3/22/05



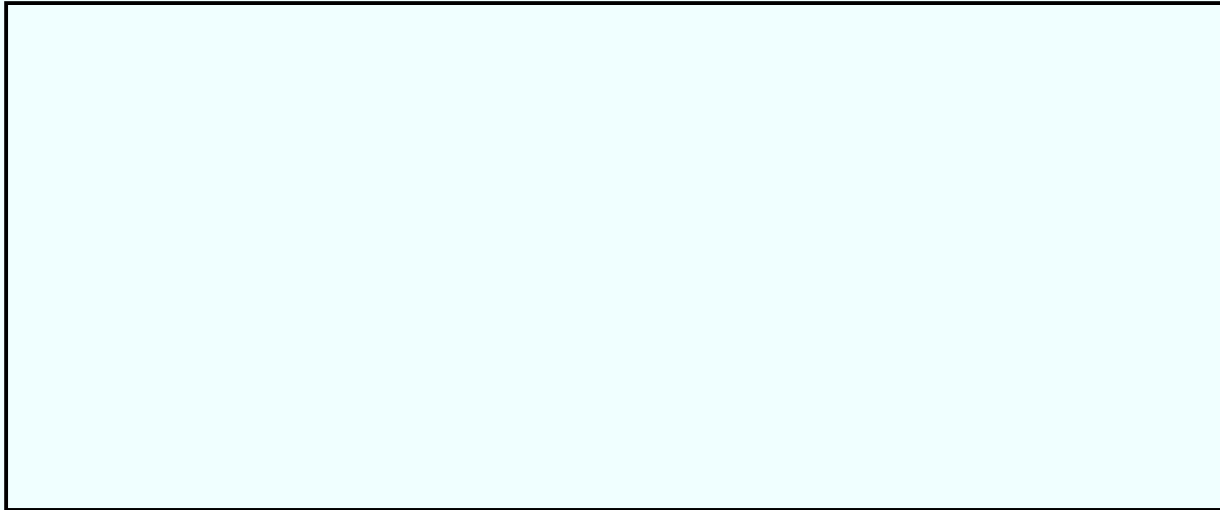
b5

REVISED 3/22/05

ADDITIONAL TOOLS TO FIGHT TERRORISM

As I have described above, the PATRIOT Act has been invaluable in providing the FBI with tools that it needs to fight terrorism in the 21st Century. This committee has been one of our strongest supporters in this effort and for this the men and women of the FBI are grateful. Having said that, I would like to address two areas in which the FBI needs the committee's support in order to continue to fulfill its primary mission of protecting America from further terrorist attacks.

b5



b5

Administrative Subpoenas

[REDACTED]

Planning, funding, supporting and committing acts of terrorism all are federal crimes. For many years, the FBI has had administrative subpoena authority for investigations of crimes ranging from drug trafficking to health care fraud to child exploitation. Yet, when it comes to terrorism investigations, the FBI has no such authority.

Instead, we rely on two tools – National Security Letters (NSLs) and orders for FISA business records. Although both are useful and important tools in our national security investigations, administrative subpoena power would greatly enhance our abilities to obtain information. Information that may be obtained through an NSL is limited in scope and currently there is no enforcement mechanism. FISA business record requests require the submission of an application for an order to the FISA Court. In investigations where there is a need to obtain information expeditiously [REDACTED]

b5

[REDACTED]

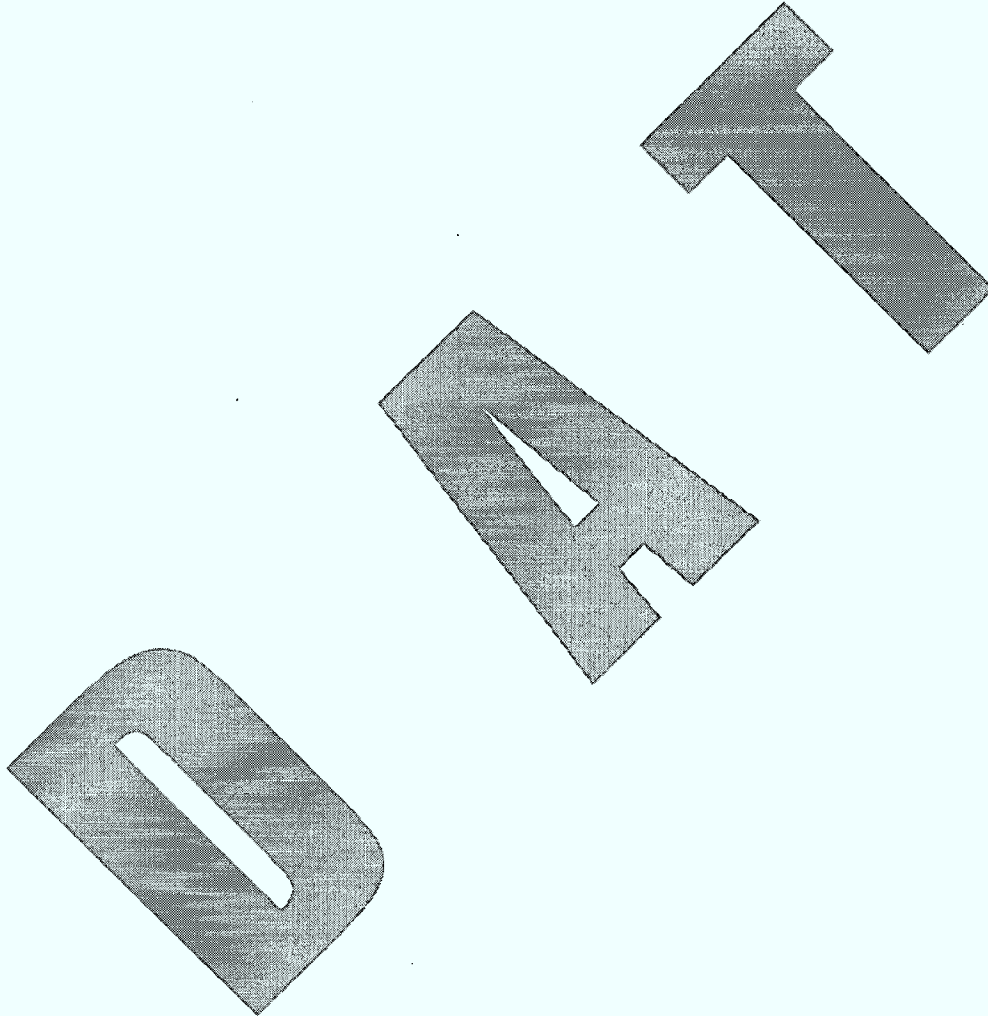
The administrative subpoena power would be a valuable complement to these tools and provide added efficiency to the FBI's ability to investigate and disrupt terrorism operations and our intelligence gathering efforts. It would provide the government with an enforcement mechanism which currently does not exist with NSLs. Moreover, it would bring the authorities of agents and analysts investigating terrorism into line with the authorities the FBI already has to combat other serious crimes. I would like to stress that the administrative subpoena power proposal could provide the recipient the ability to quash the subpoena on the same grounds as a grand jury subpoena.

CONCLUSION

Mr. Chairman and Members of the Committee, the importance of the provisions of the PATRIOT Act I have discussed today in the war against terrorism cannot be overstated. They are crucial to our present and future successes. By responsibly using the statutes

REVISED 3/22/05

provided by Congress, the FBI has made substantial progress in its ability to proactively investigate and prevent terrorism and protect lives, while at the same time protecting civil liberties. In renewing those provisions scheduled to “sunset” at the end of this year, Congress will ensure that the FBI will continue to have the tools it needs to combat the very real threat to America posed by terrorists and their supporters. In addition, by granting further modifications to the Foreign Intelligence Surveillance Act and by giving the FBI administrative subpoena authority, Congress will enable the FBI to be more efficient in its Counterterrorism efforts. Thank you for your time today.



REVISED 3/21/05

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-01-2005 BY 65179 DMH /JHF 05-CV-0845

**FBI
Office of General Counsel
National Security Law Branch**

March 21, 2005

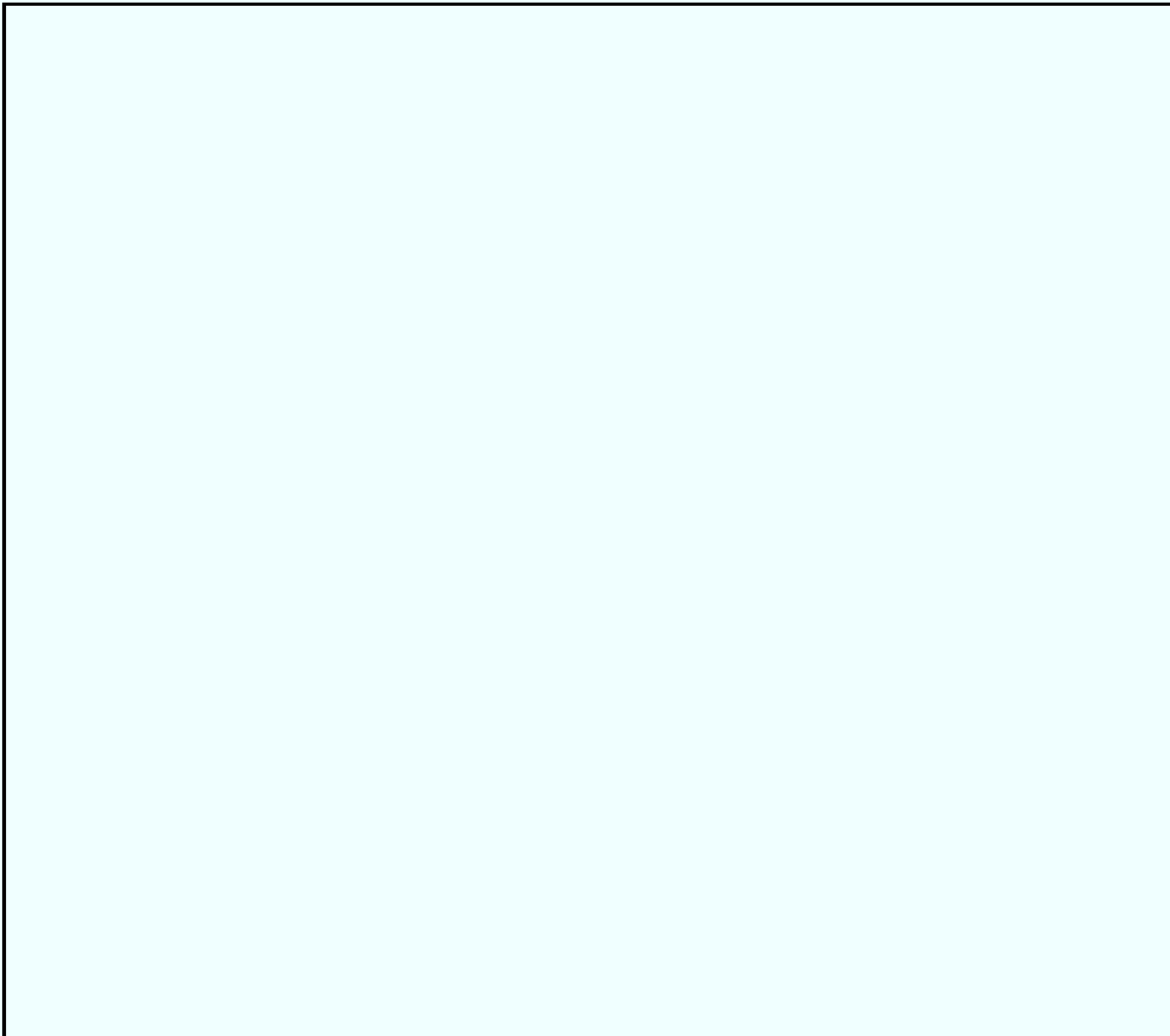
The Office of General Counsel has prepared this draft testimony at the request of the Office of Congressional Affairs. This request was received by the author of the draft on March 16, 2005 and the author was required to complete this draft on March 21, 2005. The Office of General Counsel does not have access to the full library of testimony given on this subject and must rely on the Office of Congressional Affairs to ensure that all testimony is consistent with prior testimony given by the Director and other senior FBI officials. The Office of General Counsel has requested that the Counterterrorism Division's International Terrorism Operations Sections I & II provide specific examples for use in this testimony. Such examples have not yet been received by the Office of General Counsel. The author of this draft testimony has therefore relied upon the examples from prior FBI testimony and DOJ reports to Congress.

b5

DRAFT

REVISED 3/21/05

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-01-2005 BY 65179 DMH / JHF 05-CV-0845



b5

REVISED 3/21/05

b5

REVISED 3/21/05



b5

REVISED 3/21/05

b5

ADDITIONAL TOOLS TO FIGHT TERRORISM

As I have described above, the PATRIOT Act has been invaluable in providing the FBI with tools that it needs to fight terrorism in the 21st Century. This committee has been one of our strongest supporters in this effort and for this the men and women of the FBI are grateful. Having said that, I would like to address two areas in which the FBI needs the committee's support in order to continue to fulfill its primary mission of protecting America from further terrorist attacks.

b5

REVISED 3/21/05

b5

Administrative Subpoenas

[REDACTED]
Planning, running, supporting and committing acts of terrorism are all federal crimes. For many years, the FBI has had administrative subpoena authority for investigations of crimes ranging from drug trafficking to health care fraud to child exploitation. Yet, when it comes to terrorism investigations, the FBI has no such authority.

b5

REVISED 3/21/05

Instead, we rely on two tools – National Security Letters (NSLs) and orders for FISA business records. Although both are useful and important tools in our national security investigations, administrative subpoena power would greatly enhance our abilities to obtain information. Information that may be obtained through an NSL is limited in scope and currently there is no enforcement mechanism. FISA business record requests require the submission of an application for an order to the FISA Court. In investigations where there is a need to obtain information expeditiously this may not be the most effective process to undertake. The administrative subpoena power would be a valuable complement to these tools and provide added efficiency to the FBI's ability to investigate and disrupt terrorism operations and our intelligence gathering efforts. It would provide the government with an enforcement mechanism which currently does not exist with NSLs. Moreover, it would bring the authorities of agents and analysts investigating terrorism into line with the authorities the FBI already has to combat other serious crimes. I would like to stress that the administrative subpoena power proposal could provide the recipient the ability to [redacted] quash the subpoena on the same grounds as a grand jury subpoena can be quashed [redacted]

b5

CONCLUSION

Mr. Chairman and Members of the Committee, the importance of the provisions of the PATRIOT Act I have discussed today in the war against terrorism cannot be overstated. They are crucial to our present and future successes. By responsibly using the statutes provided by Congress, the FBI has made substantial progress in its ability to proactively investigate and prevent terrorism and protect lives, while at the same time protecting civil liberties. In renewing those provisions scheduled to "sunset" at the end of this year, Congress will ensure that the FBI will continue to have the tools it needs to combat the very real threat to America posed by terrorists and their supporters. In addition, by granting further modifications to the Foreign Intelligence Surveillance Act and by giving the FBI administrative subpoena authority, Congress will enable the FBI to be more efficient in its Counterterrorism efforts. Thank you for your time today.

From: Caproni, Valerie E. (OGC) (FBI)
Sent: Tuesday, March 29, 2005 2:42 PM
To: [REDACTED] (OCA) (FBI)
Cc: [REDACTED] (OCA) (FBI)
Subject: RE: AG Statement - Patriot Act 215 Language

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-01-2005 BY 65179 DMH / JHF 05-CV-0845

b6
b7C

UNCLASSIFIED
NON-RECORD

3 comments:

[REDACTED]

b5

-----Original Message-----

From: [REDACTED] (OCA) (FBI)
Sent: Tuesday, March 29, 2005 11:26 AM
To: Caproni, Valerie E. (OGC) (FBI)
Cc: [REDACTED] (OCA) (FBI)
Subject: AG Statement - Patriot Act 215 Language

b6
b7C

UNCLASSIFIED
NON-RECORD

[REDACTED]

b5
b6
b7C

UNCLASSIFIED

UNCLASSIFIED

~~SECRET~~

TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

Testimony of Robert S. Mueller, III
Director, Federal Bureau of Investigation
Before the United States Senate
Committee on the Judiciary
Sunset Provisions of the USA Patriot Act

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 12-12-2005
CLASSIFIED BY 65179dmh/baw 05-cv-0845
REASON: 1.4 (C)
DECLASSIFY ON: 12-12-2030

April 5, 2004

Good morning Mr. Chairman, Senator Leahy and Members of the Committee. I am pleased to be here today with the Attorney General to talk with you about the ways in which the USA Patriot Act has assisted the FBI with its efforts in the war on terror. For almost three and a half years, the USA Patriot Act has changed the way the FBI operates. Many of our counterterrorism successes are the direct result of the provisions of the Act. As you know, several of these provisions are scheduled to "sunset" at the end of this year. I firmly believe that it is crucial to our national security to keep these provisions intact. Without them, the FBI might well be forced into pre-September 11th practices, requiring us - agents, analysts and our partners - to fight the war on terror with one hand tied behind our back.

[REDACTED]

[REDACTED]

b5

PATRIOT ACT SUNSET PROVISIONS

Section 201 & 202 - Expanded Title III predicates

These provisions expanded the predicate offenses for Title III intercepts to include crimes relating to chemical weapons (18 U.S.C. § 229), terrorism (18 U.S.C. §§ 2332, 2332a, 2332b, 2332d, 2339A, and 2339B), and felony violations of computer fraud and abuse (18 U.S.C. § 1030). Later amendments to this portion of the statute expanded the Title III predicates to also include 18 U.S.C. § 2232f (Bombings of places of public use, Government facilities, public transportation systems and infrastructure facilities) and 2339C (terrorism financing).

Section 201 brought the federal wiretap statute into the 21st century. Prior to its passage, law enforcement was not authorized to conduct electronic surveillance when investigating crimes committed by terrorists, such as chemical weapons offenses, killing U.S. nationals abroad, using weapons of mass destruction, and providing material support to terrorist organizations. Section 201 closed an existing gap in the Title III statute. Now Agents are able to gather information when looking into the full range of terrorism related crimes.

Section 203 (b) & (d) - Information sharing for foreign intelligence obtained in a Title III

TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

~~SECRET~~

TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

and criminal investigations.

Section 203(b) authorizes the sharing of foreign intelligence information obtained in a Title III electronic surveillance with other federal officials, including intelligence officers, DHS/DOD/ICE officials, and national security officials. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

b5

[REDACTED] Section 203(d) authorizes the sharing of foreign intelligence information collected in a criminal investigation with intelligence officials.

The information sharing provisions are overwhelmingly heralded by FBI Field Offices as the most important provisions in the Patriot Act. The ability to share critical information has significantly altered the entire manner in which terrorism investigations are conducted, allowing for a much more coordinated and effective approach than prior to the Patriot Act. Specifically, the Field Offices note that these provisions enable case agents to involve other agencies in investigations resulting in a style of teamwork that enables more effective and responsive investigations; improves the utilization of resources allowing a better focus on the case; allows for follow-up investigations by other agencies when the criminal subject leaves the U.S.; and helps prevent the compromise of foreign intelligence investigations.

Even though the law prior to the Patriot Act provided for some exchange of information, the law was complex and as a result, agents often erred on the side of caution and refrained from sharing the information. The information sharing abilities, due in part to Section 203, eliminated that hesitation and allow agents to more openly work with other government entities resulting in a much stronger team approach. Such an approach is necessary in order to effectively prevent and detect the complex web of terrorist activity. As a result, the field offices report enhanced FBI liaison with State, Local and other Federal agencies, resulting in better relationships. Even Legats notice improved relationships with intelligence agencies. If even a portion of the information sharing capabilities are allowed to 'sunset' or terminate, then the element of uncertainty is re-introduced and agents will again hesitate and take the time necessary to seek clarification of the information sharing restrictions prior to sharing information. This hesitation will lead to less teamwork and much less efficiency.

Experience has taught the FBI that there are no neat dividing lines that distinguish criminal, terrorist, and foreign intelligence activity. Criminal, terrorist and foreign intelligence

TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

~~SECRET~~
TREAT AS CLASSIFIED - SECRET
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

organizations and acts are often interrelated or interdependent. FBI files are full of examples of investigations where information sharing between counterterrorism, counterintelligence and criminal intelligence efforts and investigations was essential to the FBI's ability to protect the United States from terrorists, foreign intelligence activity and criminal activity. Some cases that start out as criminal cases become counterterrorism cases. Some cases that start out as counterintelligence cases become criminal cases. Sometimes the FBI must initiate parallel criminal and counterterrorism or counterintelligence cases to maximize the FBI's ability to adequately identify, investigate and address a variety of threats to the United States. The success of these cases is entirely dependent on the free flow of information between the respective investigations, investigators and analysts.

Ongoing criminal investigations of transnational criminal enterprises involved in counterfeiting goods, drug/weapons trafficking, money laundering and other criminal activity depend on close coordination and information sharing with the FBI's Counterterrorism and Counterintelligence Programs, as well as the Intelligence Community, when intelligence is developed which connects these criminal enterprises to terrorism, the material support of terrorism or state sponsored intelligence activity. In one such case, information from a criminal Title III and criminal investigation was passed to Counterterrorism, as well as [REDACTED] because the subject of the criminal case had previously been targeted by [REDACTED] agencies. Information sharing permitted each agency to pool their information and resources to investigate the interplay of criminal and foreign intelligence activity. [REDACTED]

b5

b5

In one instance, a terrorism case initiated in Minneapolis was subsequently transferred to San Diego and converted to a criminal case. The investigation focused on a group of Pakistan-based individuals who were involved in arms trafficking, the production and distribution of multi-ton quantifies of hashish and heroin, and the discussion of an exchange of a large quantity of drugs for four stinger anti-aircraft missiles to be used by Al Qaeda in Afghanistan. The

~~SECRET~~
TREAT AS CLASSIFIED - SECRET
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

operation resulted in the arrest, indictment and subsequent deportation of the subjects from Hong Kong to San Diego to face drug charges and charges of providing material support to Al Qaeda.

b5

Criminal enterprises are also frequently involved in, allied with or otherwise rely on smuggling operations. Alien smugglers frequently use the same routes used by drug and contraband smugglers and do not limit their smuggling to aliens, smuggling anything or anyone for the right price. Terrorists can take advantage of these smuggling routes and smuggling enterprises to enter the U.S. and are willing to pay top dollar to smugglers. Intelligence developed in these cases also frequently identifies corrupt U.S. and foreign officials who facilitate smuggling activities. Current intelligence, based on information sharing between criminal, counterterrorism, and counterintelligence efforts, has determined smugglers, as well as illegitimate and quasi-legitimate business operators in the United States, who use the services of illegal aliens.

b5

In the aftermath of the September 11th attacks, a reliable intelligence asset identified a naturalized U.S. citizen [redacted] as a leader among a group of Islamic extremists residing in the U.S. The subject's extremist views, affiliations with other terrorism subjects, and his heavy involvement in the stock market increased the potential that he was a possible financier and material supporter of terrorist activities. Early in the criminal investigation it was confirmed that the subject had developed a complex scheme to defraud multiple brokerage firms of large amounts of money. The subject was arrested and pled guilty to wire fraud. The close interaction between the criminal and intelligence cases was critical to the successful arrest of the subject before he left the country and the eventual outcome of the case.

b5

Section 204 - Clarification of Intelligence Exceptions from Limitations on Interception and Disclosure of Wire, Oral and Electronic Communications

b5

TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION



b5

Section 206 - Roving FISA Surveillance

With this provision, when a FISA target's actions have the effect of thwarting surveillance, such as by rapidly switching cell phones, Internet accounts, or even meeting venues, the Court can issue an order directing as yet unknown cell phone carrier [redacted] to effect the authorized electronic surveillance. This allows the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the Court for a new secondary order.

(S)

b5
b1

Section 206 has been extremely helpful especially in regard to IT and FCI investigations where targets move quickly and often act evasively to avoid detection. Field offices have observed counterintelligence targets change services for hard-line telephones [redacted] and cell phones numerous times. The roving authority allows them to continuously monitor these targets without interruption. By minimizing the need to return to the court for additional authorizations, it also has allowed agents to more expeditiously conclude investigations [redacted]

b5
b1

In one case, a roving FISA on a subject's cellular telephone was approved for the subject of a counterintelligence investigation who, per the usage of tradecraft, is directed to change his cellular phone every four to six months. The roving FISA allows us to continue coverage on all cell phones the subject obtains.



b5

Section 207 - Extended Duration for Certain FISAs

TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

Section 207 extends the standard duration for several categories of FISA orders. Before the passage of the USA Patriot Act, FISA orders for electronic surveillance targeted against agents of a foreign power had a maximum duration of ninety days and could be extended in 90-day increments, and orders for a physical search could be issued for no more than forty-five days, unless the target was a foreign power, in which case, the order could be issued for one year. This provision allows orders for physical searches to be issued for certain agents of foreign powers, including United States persons, for ninety days, and authorizes longer periods of searches and electronic surveillance for certain categories of foreign powers and agents of foreign powers that are not United States persons. Specifically, initial orders authorizing searches and electronic surveillance can be for periods of 120 days, and renewal orders can be extended for up to one year.

Section 207 has led to reduced paperwork in certain categories of cases. In addition, it has resulted in a more effective utilization of available personnel resources and the collection mechanisms authorized under FISA. It has allowed agents to focus their efforts on more significant and complicated terrorism-related cases and to spend more time ensuring that appropriate oversight is given to investigations involving the surveillance of United States persons.

Section 209 - Seizure of Voice Mail with a Search Warrant

Section 209 clarified that voice mail could be obtained with a search warrant under 18 U.S.C. § 2703 (similar to e-mail). Previously, some courts had required a Title III order to obtain stored voice mail. [REDACTED]

[REDACTED]

Section 209 of the USA PATRIOT Act has modernized federal law by enabling investigators to access more quickly suspects' voice-mail by using a search warrant. The speed with which voice-mail is seized and searched can often be critical to an investigation

[REDACTED]

b5

Section 212 - Emergency Disclosures of E-mail & Records by ISPs

TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

~~SECRET~~
TREAT AS CLASSIFIED -
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

Section 212 created a provision that allows a service provider (such as an Internet Service Provider) to voluntarily provide the content and records of communications related to a subscriber if it involves an emergency related to death or serious injury.

Service providers have voluntarily provided information on [redacted] under this provision. Such disclosures often included both e-mail content and associated records. [redacted]

(S) b5
b1

[redacted] This provision has also been utilized to quickly locate kidnaping victims, protect children in child exploitation cases, and to quickly respond to bomb and death threats.

[redacted] the Legats have also utilized this provision to assist foreign law enforcement officials with similar emergencies, such as death threats on prosecutors and other foreign officials. Where time is of the essence, giving service providers the option of revealing this information without a court order or grand jury subpoena is crucial to receiving the information quickly and preventing loss or serious injury [redacted]

b5

In one instance, an FBI Field Division received a bomb threat after hours. After clarifying that the bomb threat was to the local airport and that the FBI had until noon to meet the caller's demands, the FBI JTTF Agents began [redacted]

[redacted] An interview of the subject was conducted and the threat was determined to be non-credible by 11:00 a.m.

b5

In a kidnaping case, a 14 year old girl was abducted. As a result of the FBI's use of this provision, the suspect was quickly identified and interviewed. He admitted to picking up the girl and took agents to the truck stop where he had left her. Because of this provision, additional harm to the girl was prevented and she was returned to her family in a matter of hours. This is but one example of how essential this provision is for child abduction cases.

Section 214 - FISA Pen/Trap Authority

FISA pen/trap and trace orders [redacted] "the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an ongoing investigation to protect against international terrorism

b5

~~SECRET~~
TREAT AS CLASSIFIED -
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

~~TREAT AS CLASSIFIED - SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.” This provision eliminated the previous requirement that the application also contain specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in communications with such an agent, under specified circumstances. This provision now more closely tracks the requirements to obtain a pen/trap order under the criminal provisions set forth in 18 U.S.C. § 3123. The provision also expands the FISA pen/trap to include electronic communications (i.e. Internet), comparable to the criminal pen/trap provision.

[REDACTED] The (S) b1 b5
results from these pen/trap orders often help agents to determine links between the subjects of different terrorism investigations, identify other unknown associates of the subject, discover contacts for potential assets, and develop the subject’s personal profile. When pen/trap orders are quickly obtained, they allow agents to more quickly identify the associates tied to the subject of international terrorism investigations than if the agents were required to wait for service providers to respond to subpoenas for toll records, which can take several months. The old standard required more fact gathering to meet the threshold to obtain the pen/trap order, making this technique less effective and sometimes even preventing the use of this technique altogether if the window of opportunity was missed. The FISA pen/trap orders that have been obtained have been used on terrorism and counterintelligence cases, including cases as serious as one where the subject is believed to be attempting to procure nuclear arms.

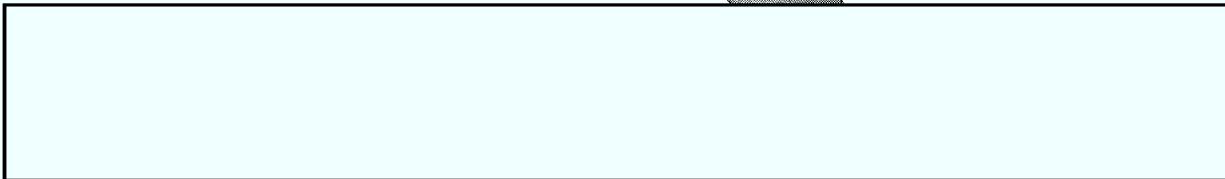
In one terrorism case, the only phone that the field office could prove was used by the subject was his associate’s phone. [REDACTED] Additionally, the field office had insufficient information that this associate was an agent of a foreign power. Thus, under the previous standard for a FISA pen/trap, the office may not have succeeded in obtaining the FISA pen/trap order. The standard established by Section 214 allowed the agents to obtain the pen/trap order by demonstrating that the information to be collected was relevant to an ongoing terrorism investigation. The information obtained by the pen/trap was valuable because it demonstrated the extent that the subject and his associate were communicating with subjects of other terrorism investigations. [REDACTED] b5 b1

[REDACTED] (S)
In another example, use of this section allowed FISA pen/trap authority based on the fact information was likely to result in foreign intelligence information. This provision allowed the field office to collect data on target lines even when the subject was out of the country and provided valuable intelligence information regarding the subject, the organization and terrorism related matters.

~~TREAT AS CLASSIFIED - SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

Section 215 - Access to Business Records under FISA

Section 215 changes the standard to compel production of business records under FISA to simple relevance (just as in the FISA pen register standard described above) and expands this authority from a limited enumerated list of certain types of business records (i.e. hotels, motels, car and truck rentals) to include "any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."



b5

Section 217 - Interception of Computer Trespasser Communications

The wiretap statute was amended to explicitly provide victims of computer attacks the ability to invite law enforcement into a protected computer to monitor the computer trespasser's communications. In the past, the law was ambiguous on this point and left open the possibility that a court could hold that a victim of computer hacking could not invite law enforcement in to monitor the intruder in an effort to prosecute and stop the intruder. The Patriot Act also established specific requirements and limitations that must be met before the use of this provision.

Under this provision, the FBI was able to monitor the communications of an international group of "carders" (individuals that use and trade stolen credit card information). The group utilized [redacted] concealed their identities [redacted]

[redacted]
[redacted]
[redacted] The owner of the hacked computer, [redacted]
[redacted] was not aware [redacted] and considered all individuals [redacted]
[redacted] to be trespassers. [redacted]

b5

[redacted] The monitoring provided leads that resulted in the discovery of the true identity of the subject. The subject was indicted in September of 2003. Without the ability to monitor these communications, it would have been unlikely that the FBI could have identified the trespassers.

~~TREAT AS CLASSIFIED - SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

Section 218 - Change in the "Primary Purpose" Standard of FISA

Section 218 changed FISA to require a certification that foreign intelligence be "a significant purpose" of the authority sought. Section 504 amended FISA to allow personnel involved in a FISA to consult with law enforcement officials in order to coordinate efforts to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities, and that such consultation does not, in itself, undermine the required certification of "significant purpose." These changes were significant to eliminate "the wall" between criminal and intelligence investigations. They now allow FBI agents greater latitude to consult criminal investigators or prosecutors without putting their FISAs at risk.

b5

As stated above, FBI field offices overwhelmingly herald the information sharing provisions as the most important provisions in the USA Patriot Act. Section 218 is an essential component to these changes. This provision [redacted] prosecutors to be involved in the earliest phases of an international terrorism investigation [redacted]

b5

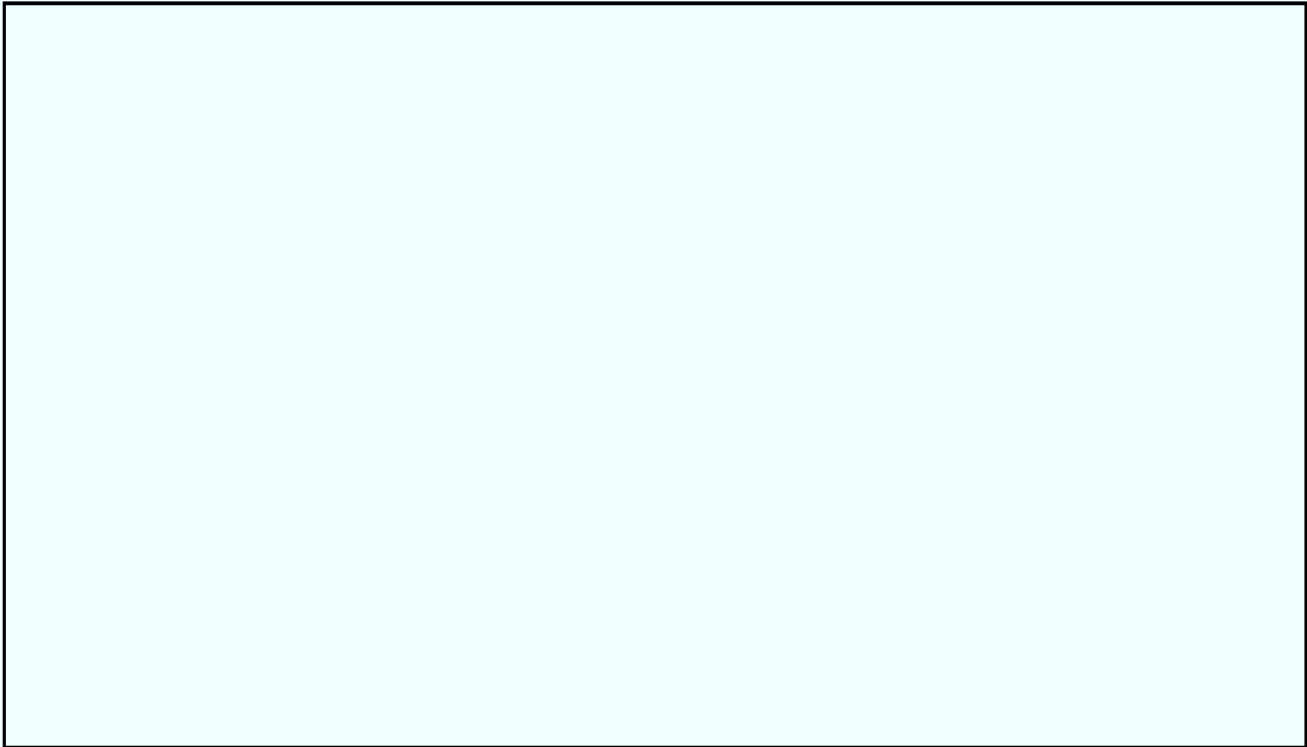
[redacted] AUSAs are often co-located with the JTTFs and are able to provide immediate input regarding the use of criminal charges to stop terrorist activity, including the prevention of terrorist attacks.

The ability to have criminal prosecutors involved in the earliest investigative phases of terrorism cases allows counterterrorism investigators to utilize the full selection of both intelligence and criminal investigative tools, enabling them to select and interchange these tools to meet the investigative demands of each particular case. Field offices are now able to use criminal prosecution, or the threat thereof, in furtherance of the intelligence objective to disrupt and dismantle terrorism, towards the ultimate goal of preventing terrorist acts. One field office notes that if 218 were allowed to "sunset," its aggressive and effective investigative approach toward terrorism would be "severely crippled."

b5

~~TREAT AS CLASSIFIED - SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

~~SECRET~~
TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION



b5

Section 220 - Nationwide Search Warrants for Electronic Evidence

Section 220 of the Act enabled courts with jurisdiction over an investigation to issue a search warrant [redacted] to compel the production of information held by a service provider, such as unopened e-mail. Previously, the search warrant had to be issued by a court in the district where the service provider was located. See 18 U.S.C. § 2703.

b5

The FBI routinely relies upon this provision when a search warrant is used to obtain the content of e-mail messages and other related information from Internet service providers (ISPs) in accordance with 18 U.S.C. § 2703. [redacted]

b5

b1

Prior to the Patriot Act, if an investigator sought a search warrant to obtain the content of un-opened e-mail from a service provider, the investigator was required to obtain this search warrant from a court in the jurisdiction where the service provider was located. To accomplish this, the case agent would brief an agent and prosecutor located in the ISP's jurisdiction on the facts of the case so that they might appear before the court and obtain the search warrant. This was a time and labor consuming process. Furthermore, because several of the largest ISPs are located in the Northern District of California [redacted] and the Eastern District of Virginia [redacted] these offices were faced with a substantial workload just to obtain search

(S)

b5

b5

~~SECRET~~
TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

~~SECRET~~
TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

warrants for other offices.

While the Patriot Act maintained the legal standard that must be met before the search warrant could be issued, that is probable cause, it eliminated the additional bureaucratic paperwork necessary to obtain that warrant in a different jurisdiction than the investigation itself. This eliminated the need to involve additional agents and prosecutors located in the same jurisdiction as the ISP. Therefore, this provision expedites the process and minimizes the labor involved without altering the privacy protection afforded the e-mail and other associated records.

Field offices repeatedly stated that this was very beneficial to quickly obtain information required in the investigation. The information obtained from these search warrants often leads to additional electronic evidence that is easily and quickly lost, therefore minimizing the time required to obtain the initial information from the ISPs is a significant asset to the investigations.

The "Virginia Jihad" case six subjects pled guilty and three were convicted of charges including conspiracy to levy war against the United States and conspiracy to provide material support to the Taliban. They received sentences ranging from a prison term of four years to life imprisonment. As a part of this case, court orders were issued to Internet Service Providers throughout the country to obtain information related to a vast number of e-mail accounts that resulted in valuable intelligence and criminal evidence used in the successful prosecution. Due to Section 220, all the court orders were issued by the district court where the prosecution occurred making the process much faster and more efficient.

This provision is regularly used in child pornography cases as agents obtain information from ISPs regarding those trading sexually exploitive images of children. This expedites the investigative process and minimizes the number of FBI, U.S. Attorney, and judicial personnel involved in the process freeing them to more aggressively pursue investigative matters.

b5

Section 223 - Civil Liability for Certain Unauthorized Disclosures

Prior to the passage of the Patriot Act, individuals were permitted only in limited circumstances to file a cause of action and collect money damages against the United States if government officials unlawfully disclosed sensitive information collected through wiretaps and electronic surveillance. Thus, while those engaging in illegal wiretapping or electronic surveillance were subject to civil liability, those illegally disclosing communications lawfully intercepted pursuant to a court order generally could not be sued. This section remedied this

~~SECRET~~
TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

~~TREAT AS CLASSIFIED - SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

inequitable situation; it created an important mechanism for deterring the improper disclosure of sensitive information and providing redress for individuals whose privacy might be violated by such disclosures.

Section 225 - Immunity for Compliance with FISA Wiretap

Pursuant to FISA, the United States may obtain wiretap or electronic surveillance orders from the FISC to monitor the communications of an entity or individual as to whom the court, among other things, finds probable cause to believe is a foreign power or the agent of a foreign power, such as international terrorists and spies. Generally, however, as in the case of criminal wiretaps and electronic surveillance, the United States requires the assistance of private communications providers, such as telephone companies [redacted] to carry out such court orders. Prior to the passage of the Patriot Act, while those assisting in the implementation of criminal wiretaps were provided with immunity, no similar immunity protected those companies and individuals assisting the government in carrying out wiretap and surveillance orders issued by the FISC under FISA. This section ended this anomaly in the law by immunizing from civil liability communications service providers and others who assist the United States in the execution of such FISA surveillance orders, thus helping to ensure that such entities and individuals will comply with orders issued by the FISC without delay.

b5

In an FBI Field Office, a case agent was able to convince [redacted] to assist in the installation of technical equipment [redacted] pursuant to a FISA order by providing a letter outlining the immunity from civil liability associated with complying with the FISA order. The target was an espionage subject. [redacted]

b5

Section 213 - Delayed Notice Search Warrants

While not scheduled to sunset, the Patriot Act's delayed notice provision Section 213 has been the subject of criticism and various legislative proposals. The FBI [redacted] believe that Section 213 is an invaluable tool in the war on terror and our efforts to combat serious criminal conduct. It is important to note that delayed notice warrants were not created by the Patriot Act. Rather, the Act simply codified a common law practice recognized by courts across the country and created a uniform nationwide standard for the issuance of those warrants [redacted] ensures that delayed notice search warrants are evaluated under the same criteria across the nation. Like any other search warrant, a delayed notice search warrant is issued by a federal judge only upon a showing that there is probable cause to believe that the property to be searched for or seized constitutes evidence of a criminal offense. A delayed notice

b5

~~TREAT AS CLASSIFIED - SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

warrant differs from an ordinary search warrant only in that the judge specifically authorizes the law enforcement officers executing the warrant to wait for a limited period of time before notifying the subject of the search that a search had been executed.

Delayed notice search warrants provide a crucial option to law enforcement and can only be requested if one of five narrowly tailored circumstances is present. The FBI has requested this authority in several cases. In most instances, the FBI seeks delayed notice when contemporaneous notice would reasonably be expected to cause serious jeopardy to an ongoing investigation.

ADDITIONAL TOOLS TO FIGHT TERRORISM

As I have described above, the PATRIOT Act has been invaluable in providing the FBI with tools that it needs to fight terrorism in the 21st Century. This committee has been one of our strongest supporters in this effort and for this the men and women of the FBI are grateful. Having said that, I would like to address two areas in which the FBI needs the committee's support in order to continue to fulfill its primary mission of protecting America from further terrorist attacks.

b5

TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

b5

Administrative Subpoenas

b5

Planning, funding, supporting and committing acts of terrorism all are federal crimes. For many years, the FBI has had administrative subpoena authority for investigations of crimes ranging from drug trafficking to health care fraud to child exploitation. Yet, when it comes to terrorism investigations, the FBI has no such authority.

Instead, we rely on two tools – National Security Letters (NSLs) and orders for FISA business records. Although both are useful and important tools in our national security investigations, administrative subpoena power would greatly enhance our abilities to obtain information. Information that may be obtained through an NSL is limited in scope and currently there is no enforcement mechanism. FISA business record requests require the submission of an

TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

~~SECRET~~
TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

application for an order to the FISA Court. In investigations where there is a need to obtain information expeditiously [REDACTED]

b5

The administrative subpoena power would be a valuable complement to these tools and provide added efficiency to the FBI's ability to investigate and disrupt terrorism operations and our intelligence gathering efforts. It would provide the government with an enforcement mechanism which currently does not exist with NSLs. Moreover, it would bring the authorities of agents and analysts investigating terrorism into line with the authorities the FBI already has to combat other serious crimes. I would like to stress that the administrative subpoena power proposal could provide the recipient the ability to quash the subpoena on the same grounds as a grand jury subpoena.

CONCLUSION

Mr. Chairman and Members of the Committee, the importance of the provisions of the PATRIOT Act I have discussed today in the war against terrorism cannot be overstated. They are crucial to our present and future successes. By responsibly using the statutes provided by Congress, the FBI has made substantial progress in its ability to proactively investigate and prevent terrorism and protect lives, while at the same time protecting civil liberties. In renewing those provisions scheduled to "sunset" at the end of this year, Congress will ensure that the FBI will continue to have the tools it needs to combat the very real threat to America posed by terrorists and their supporters. In addition, [REDACTED]

b5

[REDACTED] by giving the FBI administrative subpoena authority, Congress will enable the FBI to be more efficient in its Counterterrorism efforts. Thank you for your time today. I am happy to answer any of your questions.

~~SECRET~~
TREAT AS CLASSIFIED - ~~SECRET~~
THIS DOCUMENT HAS NOT BEEN REVIEWED FOR CLASSIFICATION

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 4
Page 22 ~ Referral/Direct
Page 23 ~ Referral/Direct
Page 24 ~ Referral/Direct
Page 25 ~ Referral/Direct

#1017326

**USA PATRIOT Act
Reauthorization Briefing Book
Valerie E. Caproni
General Counsel
Senate Judiciary Committee**

TABLE OF CONTENTS

TAB 1	Director Mueller's April 5, 2005 Testimony to the Senate Judiciary Committee Attorney General Gonzales' April 5, 2005 Testimony to the Senate Judiciary Committee
TAB 2	Transcript: April 5, 2005 Senate Judiciary Hearing on the PATRIOT Act
TAB 3	USA PATRIOT Sunset Provisions Matrix
TAB 4	Probable Cause EC, 9/16/02 Relevance v. Probable Cause Standard – Section 215 (Specter) <u>Illinois v. Gates</u> Decisions (full text)
TAB 5	Draft of FISA Improvements Act of 2005
TAB 6	NSL Statistics Grid for 10/26/01 to 12/31/04 Sample NSL EC and Draft Letter
TAB 7	NSL Semiannual Reports for Phone Records
TAB 8	NSL Semiannual Reports for Bank Records
TAB 9	NSL Semiannual Reports for Financial and Credit Reports
TAB 10	(REMOVED)
TAB 11	Section 215 Business Records Memorandum from [REDACTED] to Valerie Caproni, April 1, 2004
TAB 12	Section 215 Business Records Requests Chart

b6
b7C

	from OIPR, March 30, 2005
TAB 13	Section 215 Access to Business Records and Other Items Under FISA
TAB 14	215 Tweaks
TAB 15	FISA Roving Authority Requests Chart from OIPR, March 30, 2005
TAB 16	Section 206 Roving Surveillance Authority Under FISA

USA PATRIOT Act Provisions Subject to Sunset

Section	Description	Comment
201 (18 USC § 2516(1)(q))	<u>Adds to the predicate offenses for wiretaps:</u> 18 USC § 229 (chemical weapons); § 2332 (crimes of violence against Americans overseas); § 2332a (weapons of mass destruction); § 2332b (multinational terrorism); § 2332d (financial transactions with terrorist countries); § 2339A (supporting terrorists); § 2339B (supporting terrorist organizations)	Applies to Title-III wiretaps
202 (18 USC § 2516(1)(c))	<u>Adds to the predicate offenses for wiretaps:</u> 18 USC § 1030 (computer fraud & abuse)	Applies to Title-III wiretaps
203(b) (18 USC § 2517(6))	Authorizes disclosure of FI, CI and FI information acquired pursuant to Title III to law enforcement, intelligence, protective, immigration, national defense, and national security officials	
203(d) (50 USC § 403-5d)	Authorizes disclosure of FI, CI and FI information acquired in a criminal investigation to law enforcement, intelligence, protective, immigration, national defense, and national security officials	b5
204 (18 USC § 2511(2)(f))	Makes clear that the general pen register/trap & trace proscriptions do not bar execution of FISA pen register or trap & trace orders	
206 (50 USC § 1805(c)(2)(B))	"FISA roving surveillance" Authorizes FISA orders to command the assistance of individuals not specifically identified in the order in cases in which the target has taken steps to prevent the identification of specified persons	LE already had this under Title III; b5
207 (50 USC § 1805(e), 1824(d))	Extends duration of FISA orders directed against agents of a foreign power to 120 days and permits extensions at intervals of up to 1 year [up from 90 days (surveillance) & 45 days (searches) for both original orders and extensions]	
209 (18 USC § 2709; 2510(1),(14))	Makes clear that law enforcement access to voice mail requires only a search warrant	Requirements applicable to Title-III wiretaps are more restrictive than search warrants

212 (18 USC § 2702; 2703)	Permits communications service providers to disclose customer records or content of customer communications in an emergency situation involving the immediate danger of serious bodily injury	
214 (50 USC § 1842; 1843)	Authorizes FISA pen register/trap & trace orders with respect to <i>electronic</i> communications [e-mail address, URL identification (but not content)] under procedure previously limited to <i>wire</i> communications (telephone number of source and addressee); eliminates requirement that the communication either be that of terrorists or spies or related to their criminal activities	
215 (50 USC §§ 1861; 1862)	Authorizes FISA court orders for business records and other tangible items in investigations of international terrorism or espionage (or IAW PL 107-108, §314(a)(6), to obtain foreign intelligence information not concerning a US person)	Most controversial of the sunset provisions; perceived to allow the FBI to raid libraries -- no library has been searched pursuant to this provision. Court order is required (based on "relevance" to an authorized IT or CI investigation)
217 (18 USC §§ 2511(2)(i); 2510(21))	Authorizes interception of communications to/from a trespasser within a protected computer	
218 (50 USC §§ 1804(a)(7)(B); 1823(a)(7)(B))	Changes the certification required for a FISA order from "the purpose" to "a significant purpose" to collect FI information; earlier language (which would be revived at sunset) was the one basis for the "wall" between intelligence and criminal investigations	Had a lot to do with demise of "the wall" between intelligence and LE investigations; perhaps the single most productive change to FISA yet.
220 (18 USC §§ 2703; 3127)	Authorizes service anywhere in the world of a court order granting law enforcement access to the content of voice mail and e-mail communications (and/or related records) held by service providers; previously, such orders had to be issued in the place where they were to be executed	

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

MEMORANDUM

DATE: 10-24-2005
CLASSIFIED BY 65179 dmh/elh
REASON: 1.4 (c)
DECLASSIFY ON: 10-24-2030

05-cv-0845

To: General Counsel Valerie Caproni

From: Unit Chief

b6

b7C

Date: April 1, 2004

SUBJ.: Business Record Requests

b1

b3 T50 USC 1861

b6

b7C

\$215 REQUESTS APPROVED SINCE JULY 2004

(S)

(S)

(S)

(S)

(S)

(The above list I verified with at OIPR. Our branch records show the following business records as having been completed projects, although I did not verify these with OIPR. Please let me know if verification is needed.)

b6

b7C

ADDITIONAL \$215 REQUESTS

~~SECRET~~

~~SECRET~~

(S)

(S)

b1

b3 T50 USC 1861

b6

b7C

(For the above, the NSLB database does not list the type of records requested/obtained. I will obtain for you, if needed.)

PENDING REQUESTS

(S)

(S)

(S)

(S)

(S)

~~SECRET~~

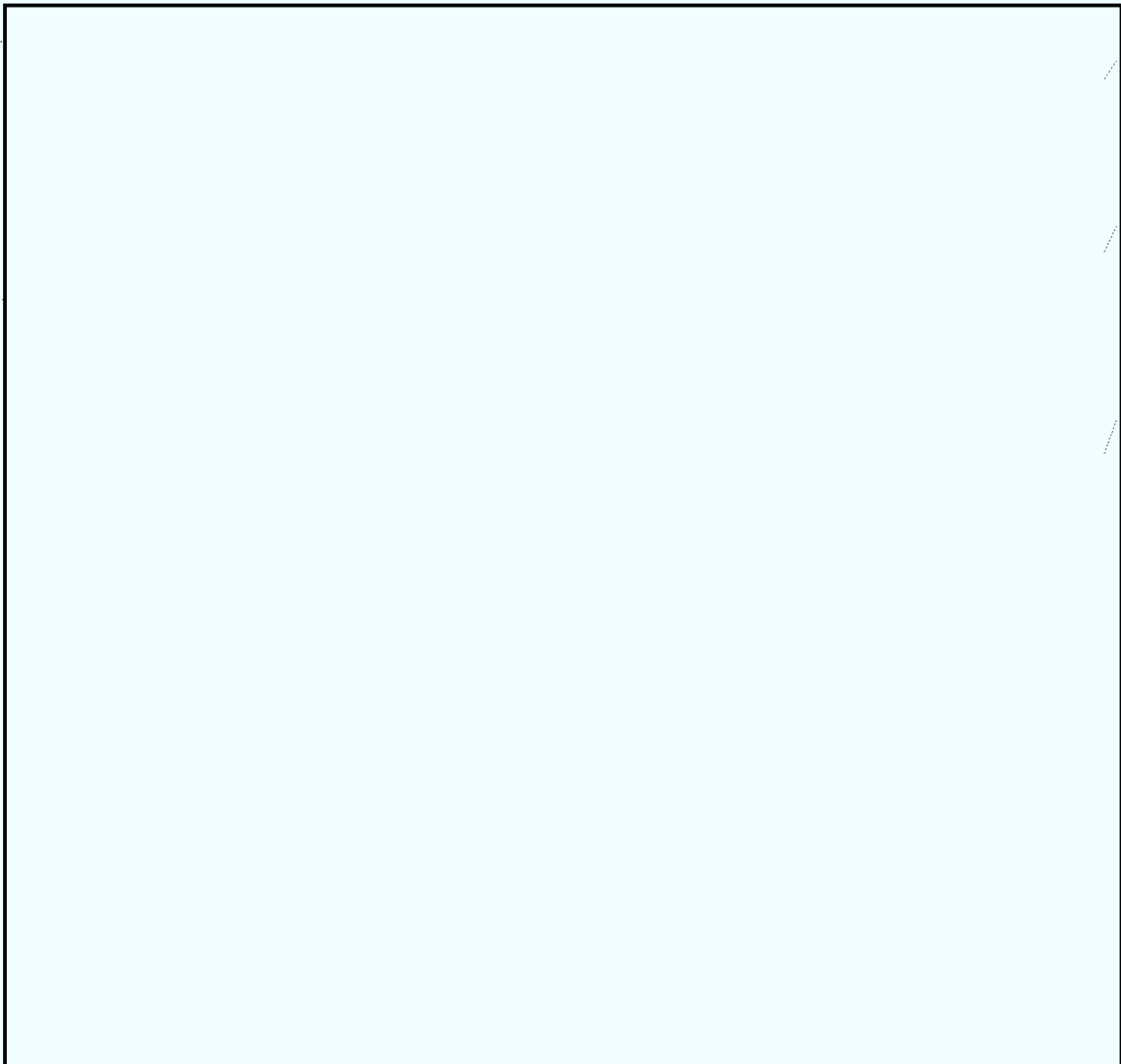
b1

b3 T50 USC 1861

b6

b7C

~~SECRET~~



(S)

(S)

(S)

(S)

(S)

(S)

b1

b3 T50 USC 1861

b6

b7C

~~SECRET~~

~~SECRET//ORCON,NOFORN~~

05-cv-0845

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 10-24-2005
CLASSIFIED BY 65179 dmh/elh
REASON: 1.4 (c)
DECLASSIFY ON: 10-24-2030

(S)

1

(S)

~~SECRET//ORCON,NOFORN~~

b1
b2
b3 T50 USC 1861
b6

~~SECRET//ORCON,NOFORN~~

(S)

~~SECRET//ORCON,NOFORN~~

b1

b2

b3 T50 USC 1861

b6

~~SECRET//ORCON,NOFORN~~

O/S



(S)

(S)

~~SECRET//ORCON,NOFORN~~

b1

b2

~~SECRET//ORCON,NOFORN~~

(S)

~~SECRET//ORCON,NOFORN~~

b1

b2

b3 T50 USC 1861

b6

~~SECRET~~//ORCON,NOFORN

(S)

~~SECRET~~//ORCON,NOFORN

b1

b2

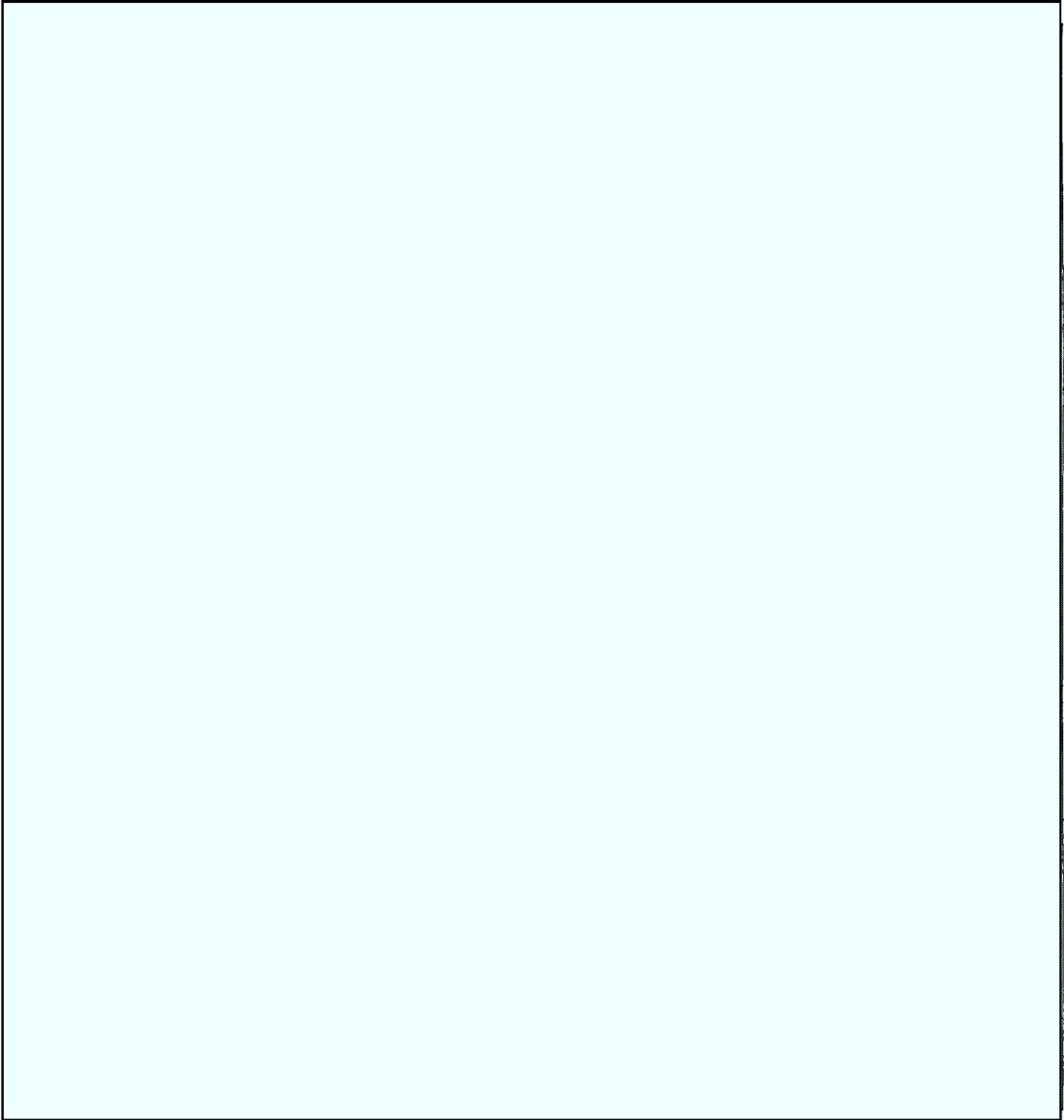
b3 T50 USC 1861

b6

~~SECRET//ORCON,NOFORN~~



(S)



~~SECRET//ORCON,NOFORN~~

b1

b2

b3 T50 USC 1861

b6

NOV 000 1 1 2

REF ID: A66777

~~SECRET~~//ORCON,NOFORN

(S)

~~SECRET~~//ORCON,NOFORN

b1

b2

b3 T50 USC 1861

b6

~~SECRET//ORCON,NOFORN~~

(S)

~~SECRET//ORCON,NOFORN~~

b1

b2

b3 T50 USC 1861

b6

~~SECRET~~//ORCON,NOFORN

(S)

~~SECRET~~//ORCON,NOFORN

b1

b2

b3 T50 USC 1861

~~SECRET~~//ORCON,NOFORN

(S)

~~SECRET~~//ORCON,NOFORN

b1

b2

b3 T50 USC 1861

~~SECRET//ORCON,NOFORN~~

(S)

~~SECRET//ORCON,NOFORN~~

b1

b2

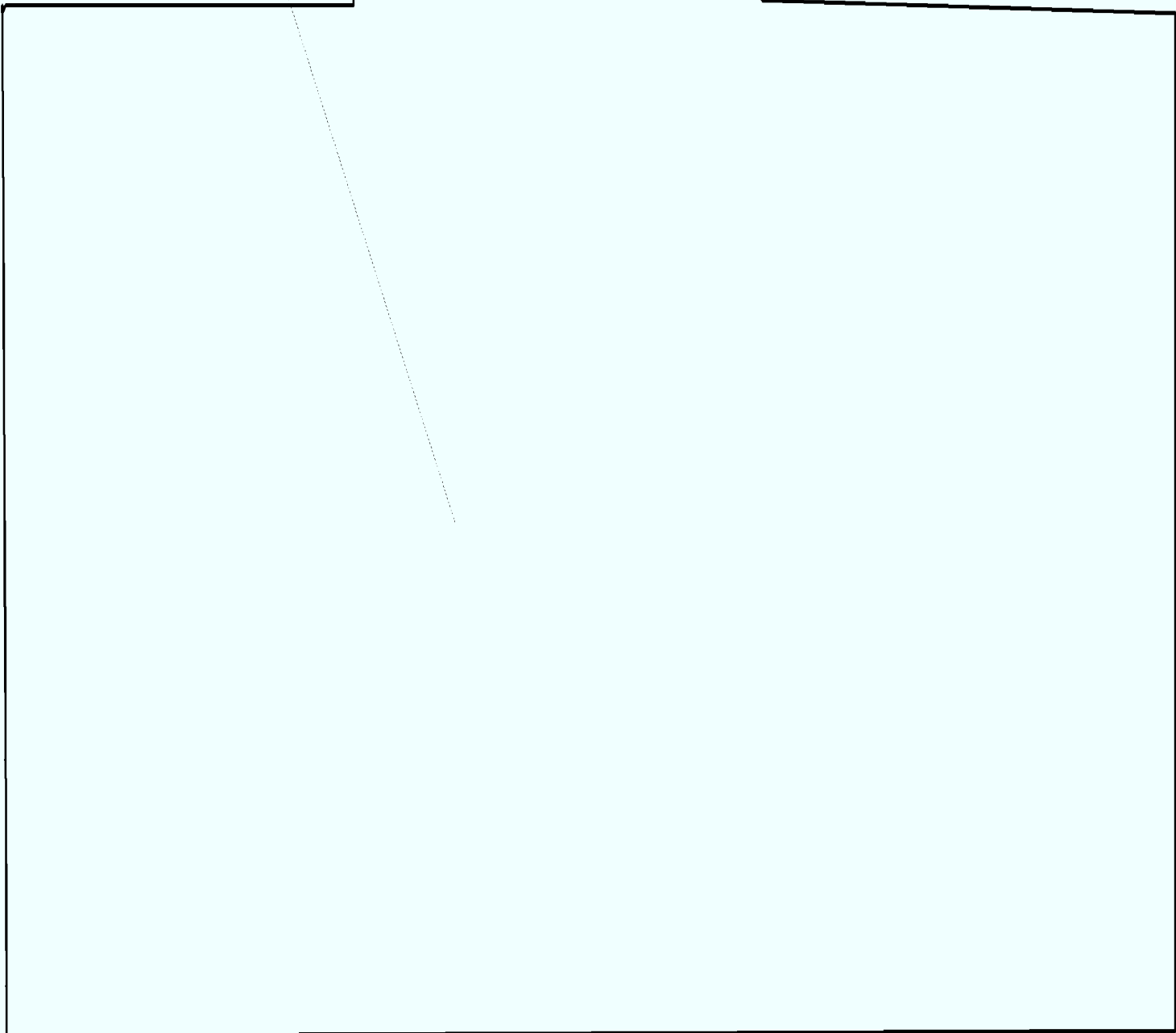
b3 T50 USC 1861

b6

~~SECRET//ORCON,NOFORN~~

(S)

12



~~SECRET//ORCON,NOFORN~~

b1

b2

b3 T50 USC 1861

b6

b7C

Section 215. Access to Business Records and Other Items under FISA

- Section 215 gives the FISA Court the authority in foreign intelligence investigations, such as those involving international terrorism and espionage, to order the production the same kinds of tangible things that prosecutors have always been able to obtain through grand-jury subpoenas in criminal investigations.
- **Before the USA PATRIOT Act**, it was difficult for investigators to obtain court orders for access to business records in connection with foreign intelligence investigations.
- Section 215 improved FISA's original business-records authority in a number of respects:
 - It expanded the **types of entities** that can be compelled to disclose information. Under the old provision, the FBI could obtain records only from "a common carrier, public accommodation facility, physical storage facility or vehicle rental facility." The new provision contains no such restrictions.
 - It expanded the **types of items** that can be requested. Under the old authority, the FBI could only seek "records." Now, the FBI can seek "any tangible things (including books, records, papers, documents, and other items)."
- Although the FISA Court could now issue a section 215 order to a library so long as a judge determined that the library possessed records relevant to an international terrorism or espionage investigation, **the provision does not single libraries out or even mention them at all**; it simply does not exempt libraries from the range of entities that may be required to produce records.
- The library habits of ordinary Americans are of **no interest** to those conducting terrorism investigations. However, historically terrorists and spies *have* used libraries to plan and carry out activities that threaten our national security. **We should not allow libraries to become safe havens for terrorist or clandestine activities.**
 - For example, Brian Regan, a former TRW employee working at the National Reconnaissance Office who recently was convicted of espionage, extensively used computers at five public libraries in Northern Virginia and Maryland to access addresses for the embassies of certain foreign governments.
 - In addition, the Justice Department has confirmed that, as recently as the winter and spring of 2004, a member of a terrorist group closely affiliated with al Qaeda used Internet service provided by a public library to communicate with his confederates.
- Obtaining business records is a long-standing law enforcement tactic. **For years, ordinary grand juries** have issued subpoenas to all manner of businesses, including libraries and bookstores, for records relevant to criminal inquiries.

- In a recent **criminal** case, a grand jury served a subpoena on a bookseller to obtain records showing that a suspect had purchased a book giving instructions on how to build a particularly unusual detonator that had been used in several bombings. This was important evidence identifying the suspect as the bomber.
- In the 1997 **Gianni Versace** murder case, a Florida grand jury subpoenaed records from public libraries in Miami Beach.
- In the 1990 **Zodiac gunman** investigation, a New York grand jury subpoenaed records from a public library in Manhattan. Investigators believed that the gunman was inspired by a Scottish occult poet, and wanted to learn who had checked out his books.
- Section 215 authorized the FISA court to issue **orders similar to grand-jury subpoenas in national-security investigations**. However, it contains a number of safeguards that protect civil liberties, and is actually **more protective of privacy** than the authorities for ordinary grand-jury subpoenas.
 - A **court must explicitly authorize** the use of section 215 through a **court order**. Agents cannot use this authority unilaterally to compel any entity to turn over its records. **By contrast, a grand jury subpoena is typically issued without any prior judicial review or approval.**
 - Section 215 **expressly protects First Amendment rights**, unlike federal grand-jury subpoenas. It explicitly provides that the FBI cannot conduct investigations “of a United States person solely on the basis of activities protected by the First Amendment to the Constitution of the United States.”
 - Section 215 has a **narrow scope**. It can only be used (1) “to obtain foreign intelligence information not concerning a United States person”; or (2) “to protect against international terrorism or clandestine intelligence activities.” **It cannot be used to investigate ordinary crimes, or even domestic terrorism.** A grand jury can obtain business records in investigations of *any* federal crime.
- Section 215 orders are also subject to the **same burden of proof as are grand-jury subpoenas**; investigators must meet a standard of relevance.
- Section 215 provides for **congressional oversight**. Every six months, the Attorney General must “fully inform” Congress on how it has been implemented. To date, the Justice Department has provided Congress with six reports regarding its use of section 215.
- **Allowing section 215 to expire would make it much harder for investigators to obtain critical evidence in international terrorism and espionage investigations.**

POSSIBLE QUESTIONS:

Isn't it true that under section 215 of the USA PATRIOT Act, the FISA court is just a rubberstamp because the judge must issue an order requiring the production of records if he or she receives an application from the Department asserting that it is seeking the records in connection with a foreign intelligence investigation, or an investigation to protect against international terrorism or clandestine intelligence activities?

- This description of section 215 is **categorically false**.
- Pursuant to section 215, a judge "shall" issue an order "approving the release of records **if the judge finds that the application meets the requirements of this section.**" 50 U.S.C. § 1861(c)(1) (emphasis added).
- As a result, before issuing an order requiring the production of any records under section 215, a federal judge must find that the requested records are sought for (and thus relevant to) "an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(b)(2).
- In addition, a federal judge must find that the investigation is not being conducted of a United States person solely on the basis of activities protected by the First Amendment. 50 U.S.C. § 1861(a)(2)(b).
- Moreover, the United States has stated in litigation that recipients of orders for the production of records under section 215 may challenge the legality of those orders in the FISA Court.

Isn't it true that section 215 orders, unlike grand-jury subpoenas, are not governed by a relevance standard?

- **Section 215 orders are subject to the same relevance standard as are grand-jury subpoenas.**
- **Just as grand-jury subpoenas may be issued to obtain records that are relevant to a criminal investigation, the FISA Court may issue orders requiring the production of records under section 215 that are relevant to an authorized international terrorism or espionage investigation.**
- Some critics have complained that section 215 does not contain a "relevance" standard because **the word "relevance" is not specifically mentioned in the provision itself.**
- Section 215, however, states that the FISA Court may only enter an order requiring the production of records if such records are "**sought for an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.**" 50 U.S.C. § 1862(a).

- **This is the equivalent of a relevance standard because if records are irrelevant to an investigation, then they are not being “sought for” that investigation.**

Isn't it true that section 215 explicitly forbids establishments such as libraries from telling their patrons that the government has requested their records? Why shouldn't libraries be able to tell their patrons when the government has requested their records?

- **The provision forbids the recipient of a section 215 order from disclosing to others that the government has requested the production of documents pursuant to section 215.**
 - Section 215, however, contains an explicit exception allowing the recipient of a section 215 order to inform those whose assistance is needed to produce the requested records.
 - The Department also takes the position that section 215 also contains an **implicit exception to the nondisclosure requirement** allowing the recipient of a section 215 order to **inform his or her attorney** of the request for the production of records.
- Such a nondisclosure requirement, however, is standard operating procedure for the conduct of surveillance in sensitive international terrorism or espionage investigations.
- **It is critical that terrorists are not tipped off prematurely about intelligence investigations. Otherwise, their conspirators may flee and key information may be destroyed before the government's investigation has been completed.**
 - As the U.S. Senate concluded when adopting the Foreign Intelligence Surveillance Act: “By its very nature, foreign intelligence surveillance must be conducted in secret.”
 - Furthermore, were information identifying the targets of international terrorism and espionage investigations revealed, according to the D.C. Circuit, such disclosures would “inform terrorists of both the substantive and geographic focus of the investigation[,] . . . would inform terrorists which of their members were compromised by the investigation, and which were not[,] . . . **could allow terrorists to better evade the ongoing investigation and more easily formulate or revise counter-efforts . . . [and] be of great use to al Qaeda in plotting future terrorist attacks or intimidating witnesses in the present investigation.**” *Center for National Security Studies v. U.S. Department of Justice*, 331 F.3d 918, 928-29 (D.C. Cir. 2003).

While the Department has claimed that section 215 of the USA PATRIOT Act is a vital tool in the war against terrorism, the Department stated in the fall of 2003 that it had yet to use this new authority. If section 215 is such an important provision, then why was it not utilized in its first two years of existence?

- **The fact that an authority may be used infrequently does not denigrate its importance.**

- To the contrary, it is important that the authority exists for situations in which a section 215 order could be critical to the success of an investigation.
 - Just as prosecutors need to obtain relevant records through grand-jury subpoenas in criminal investigations, so, too, do investigators in national-security investigations sometimes need to obtain relevant records.
- **Just as a police officer knows that his firearm may be invaluable in preventing crime, even if he cannot predict when he might need to draw it from his holster, section 215 provides investigators an authority they may find crucial to stop a terrorist plot.**
- **The fact that the Department has used this authority in a judicious manner should not be used as an argument for repealing the provision altogether.**

By restoring the requirement of “specific and articulable facts” that the records sought under FISA pertain to a terrorist, spy or other foreign agent, which merely requires some individual suspicion, wouldn’t the SAFE Act greatly limit the danger that section 215 could be misused to secretly obtain the private records of innocent people?

- The SAFE Act would require the FISA Court, before issuing an order for the production of records under section 215, to find that there are “specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.”
- The SAFE Act would therefore deny terrorism investigators access to crucial intelligence information by raising the standard under which the FISA court can order the production of **business records** and other tangible things.
 - Section 215 orders are currently governed by the same relevance standard that is currently used with respect to grand-jury subpoenas.
 - By imposing a “specific and articulable facts” standard for obtaining business records in a FISA investigation, which is much higher than the simple relevance standard for obtaining a grand-jury subpoena that is also currently used under section 215, the SAFE Act would make it much more difficult to investigate terrorists and spies than to investigate drug dealers or bank robbers.
 - Investigators, for example, would be denied access to records that are indisputably relevant to an international terrorism investigation simply because the records do not specifically pertain to the suspected terrorist.
- Section 215 already contains sufficient safeguards to guarantee that it is not misused to obtain the private records of innocent people, and it is actually *more protective of privacy* than the authorities for ordinary grand-jury subpoenas.

- A court must explicitly authorize the use of section 215 through a court order. Agents cannot use this authority unilaterally to compel any entity to turn over its records. By contrast, a grand-jury subpoena is typically issued without any prior judicial review or approval.
- Section 215 expressly protects First Amendment rights, unlike federal grand-jury subpoenas. It explicitly provides that the FBI cannot conduct investigations “of a United States person solely on the basis of activities protected by the First Amendment to the Constitution of the United States.”
- Section 215 has a narrow scope. It can only be used (1) “to obtain foreign intelligence information not concerning a United States person”; or (2) “to protect against international terrorism or clandestine intelligence activities.” It cannot be used to investigate ordinary crimes, or even domestic terrorism. A grand jury can obtain business records in investigations of any federal crime.
- Section 215 provides for congressional oversight. Every six months, the Attorney General must “fully inform” Congress on how it has been implemented. No similar oversight exists with respect to grand-jury subpoenas.

DATE: 10-24-2005
CLASSIFIED BY 65179 dmh/elh
REASON: 1.4 (c)
DECLASSIFY ON: 10-24-2030

~~SECRET//ORCON,NOFORN~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

1

(S)

(S)

~~SECRET//ORCON,NOFORN~~

b1

b2

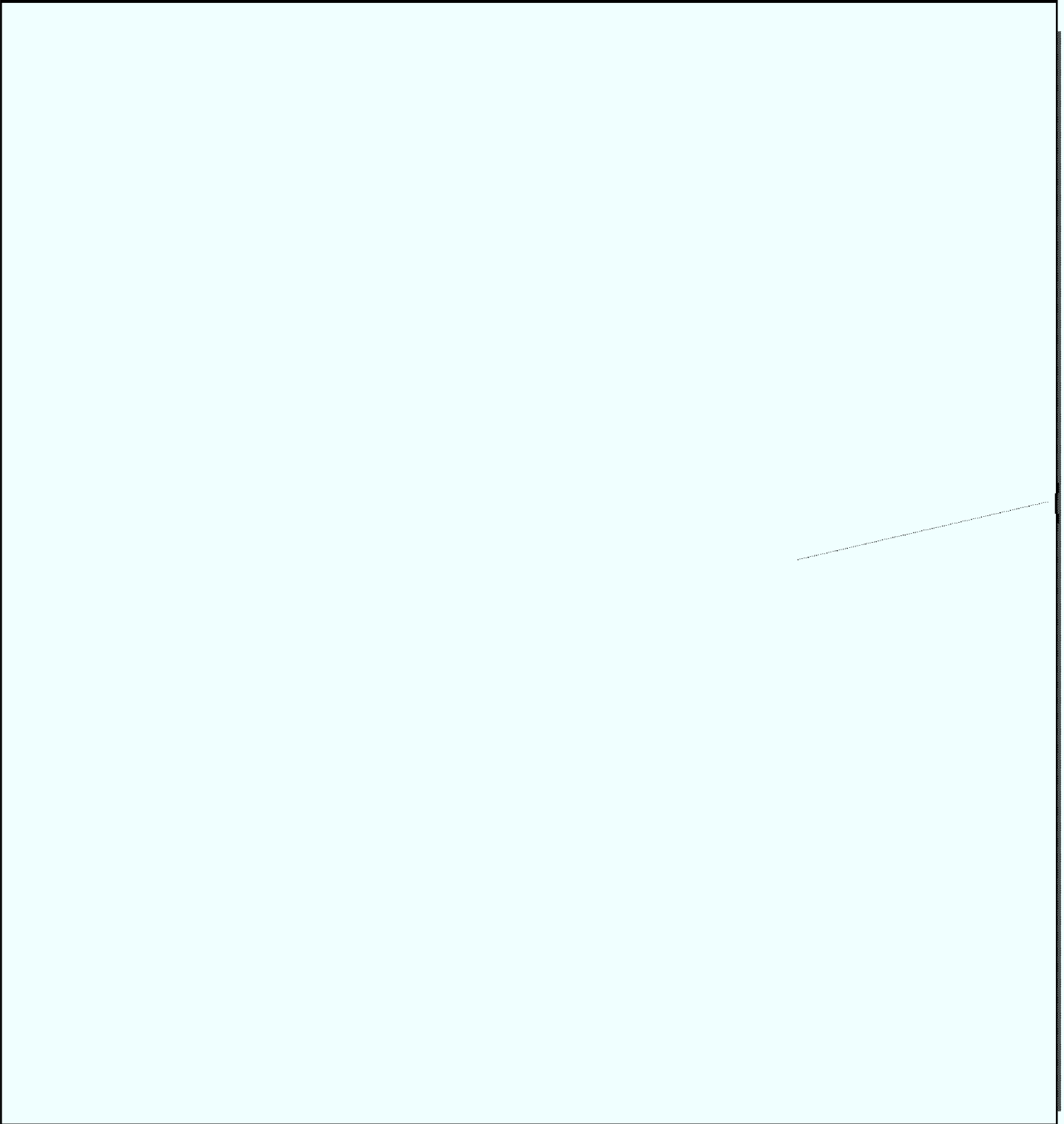
b3 T50 USC 1805

~~SECRET//ORCON,NOFORN~~



(S)

2



(S)

~~SECRET//ORCON,NOFORN~~

b1

b2

b3 T50 USC 1805

~~SECRET~~//ORCON,NOFORN



(S)

3

(S)

~~SECRET~~//ORCON,NOFORN

b1

b2

~~SECRET//ORCON,NOFORN~~



(S)

4

(S)

~~SECRET//ORCON,NOFORN~~

b1

b2

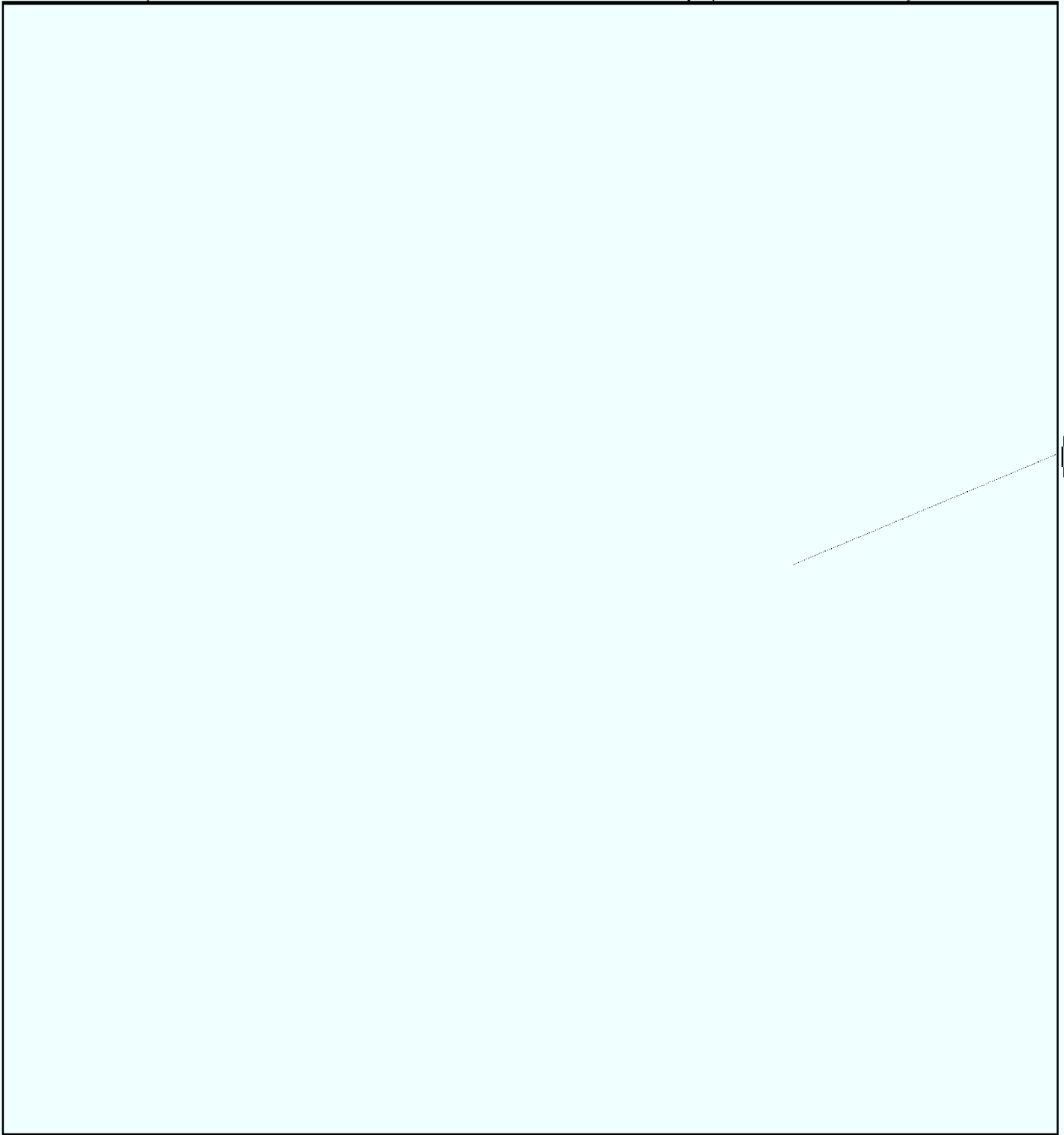
b3 T50 USC 1805

~~SECRET//ORCON,NOFORN~~



(S)

5



(S)

~~SECRET//ORCON,NOFORN~~

b1

b2

b3 T50 USC 1805

~~SECRET//ORCON,NOFORN~~



(S)

6

(S)

~~SECRET//ORCON,NOFORN~~

b1

b2

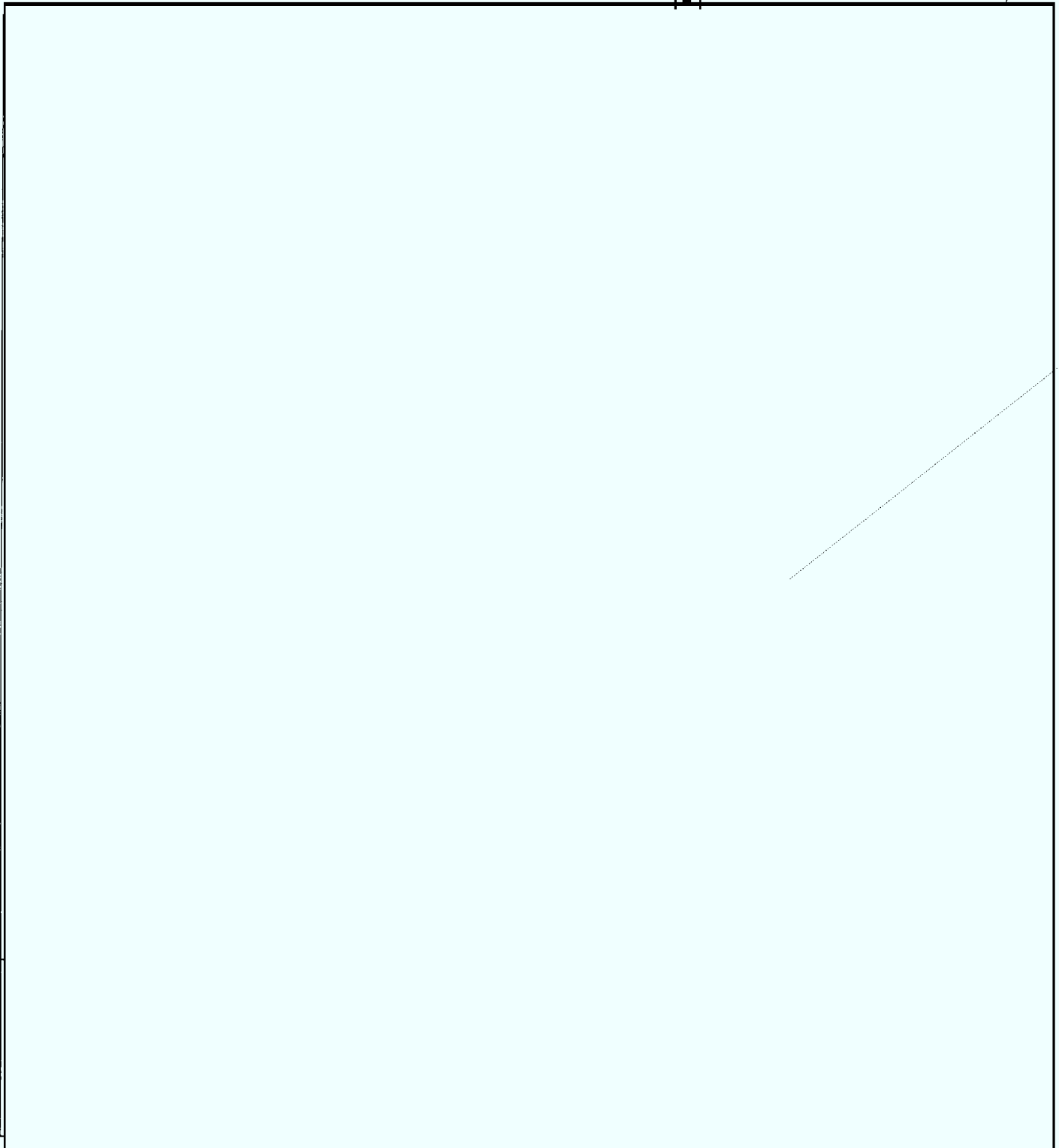
b3 T50 USC 1805

~~SECRET~~//ORCON,NOFORN



(S)

7



(S)

~~SECRET~~//ORCON,NOFORN

b1

b2

~~SECRET~~//ORCON,NOFORN

(S)

8

(S)

b1

b2

b3 T50 USC 1805

b6

b7C

~~SECRET~~//ORCON,NOFORN

Section 206. Roving Surveillance Authority Under the Foreign Intelligence Surveillance Act of 1978 ("FISA")

- Section 206 allows the FISA court to authorize "roving" surveillance of a terrorist or spy when it finds that the target's actions may thwart the identification of those specific individuals or companies, such as communications providers, whose assistance may be needed to carry out the surveillance.
- A "roving" wiretap order attaches to a particular target rather than a particular phone or other communications facility.
- **Before the USA PATRIOT Act**, the use of roving wiretaps was not available under FISA.
 - Therefore, each time a suspect changed communication providers, investigators had to return to the FISA court for a new order just to change the name of the facility to be monitored and the "specified person" needed to assist in monitoring the wiretap.
 - **International terrorists and foreign intelligence officers, however, are trained to thwart surveillance** by changing communications facilities just prior to important meetings or communications.
 - As a result, without roving wiretaps, investigators could be left two steps behind sophisticated terrorists.
- **For years, law enforcement has been able to use roving wiretaps to investigate ordinary crimes, including drug offenses and racketeering.** The authority to use roving wiretaps in traditional criminal cases has existed since 1986.
- Section 206 **simply authorized the same techniques** used to investigate ordinary crimes to be used in **national-security investigations**. This provision has put investigators in a better position to counter the actions of spies and terrorists who are trained to thwart surveillance.
- Section 206 contains a number of **privacy safeguards**.
 - Significantly, section 206 did not change the requirement that the target of roving surveillance must be identified or described in the order.
 - Therefore, section 206 is **always connected to a particular target of surveillance**. FISA nonetheless requires the government to provide "a description of the target of the electronic surveillance" to the FISA Court prior to obtaining a roving surveillance order.
 - Section 206 did not alter the requirement that before approving a roving surveillance order, the **FISA Court must find that there is probable cause** to believe the target of the surveillance is either a **foreign power or an agent of a foreign power, such as a terrorist or spy**.

b2

b7E

- Roving surveillance under section 206 can be ordered only after the FISA Court makes a finding that the actions of the target of the application may have the effect of thwarting the surveillance.
- Moreover, section 206 in no way altered the rigid FISA minimization procedures that limit the acquisition, retention, and dissemination by the government of information or communications involving United States persons.
- A number of federal courts – including the Second, Fifth, and Ninth Circuits – have squarely ruled that “**roving**” wiretaps are perfectly consistent with the Fourth Amendment. No court of appeals has reached a contrary conclusion.
- If section 206 were allowed to expire, investigators would once again often struggle to catch up to sophisticated terrorists and spies trained to take steps such as constantly changing cell phones in order to avoid surveillance.

POSSIBLE QUESTION:

Because wiretaps are the most intrusive form of surveillance known to the law, is it asking too much to require the government, when it seeks a surveillance order than can jump from telephone to telephone, [REDACTED]

- FISA currently requires an order approving electronic surveillance to specify, among other things: (1) the identity, if known, or a description of the target of the electronic surveillance; and (2) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known.
- Many civil liberties advocates have therefore complained that “roving” wiretaps under FISA may be used to violate the privacy of innocent Americans because:
 - FISA allows for the issuance of surveillance orders that **neither specify the locations** that will be placed under surveillance [REDACTED] and [REDACTED]
 - FISA does not contain any requirement that “roving” surveillance may be conducted [REDACTED] at a particular location is ascertained by the government.
- The SAFE Act seeks to correct these purported deficiencies in FISA by requiring that:
 - An electronic surveillance order under FISA specify either: [REDACTED] or (2) the location of each of the facilities or places at which surveillance will be directed; and

b2

b7E

- Proponents of the SAFE Act have claimed that this provision would simply impose the same requirement on FISA “roving” wiretap orders as are currently placed on “roving” wiretap orders issued in criminal investigations.
- This argument, however, is incorrect.
 - The specific “ascertainment” requirement contained in the criminal wiretap statute applies to the interception of oral communications, such as through bugging, and not to the interception of wire or electronic communications, such as telephone calls.
 - This provision of the criminal wiretap statute states that the interception of an oral communication “shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order.” See 18 U.S.C. § 2518(12).
 - With respect to the interception of wire or electronic communications, the criminal wiretap statute imposes a more lenient standard, requiring that surveillance can be conducted “only for such time as it is reasonable to presume that [target of the surveillance] is or was reasonably proximate to the instrument through which such communication will be or was transmitted.” See 18 U.S.C. § 2518(11)(b)(iv).
- Congress should not impose restrictions that make it more difficult for investigators to conduct roving wiretaps directed against international terrorists than it is to conduct such wiretaps against drug dealers and those participating in organized crime.
- The Department believes that FISA already contains sufficient safeguards to ensure that the government does not intrude on the privacy of innocent Americans.
 - The target of roving surveillance must be identified or described in the order of the FISA Court. A roving wiretap order is therefore [REDACTED] of surveillance. b2 b7E
 - The FISA Court must find that there is probable cause to believe the particular target of the surveillance is either a foreign power or an agent of a foreign power, such as a terrorist or spy.
 - Roving surveillance can be ordered only after the FISA court makes a finding that the actions of the target of the application may have the effect of thwarting the surveillance.
 - FISA requires the use of robust minimization procedures that limit the acquisition, retention, and dissemination by the government of information or communications involving United States persons.

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 20

Page 314 ~ Duplicate

Page 315 ~ Duplicate

Page 316 ~ Duplicate

Page 317 ~ Duplicate

Page 318 ~ Duplicate

Page 319 ~ Duplicate

Page 320 ~ Duplicate

Page 321 ~ Duplicate

Page 322 ~ Duplicate

Page 323 ~ Duplicate

Page 324 ~ Duplicate

Page 325 ~ Duplicate

Page 326 ~ Duplicate

Page 327 ~ Duplicate

Page 328 ~ Duplicate

Page 329 ~ Duplicate

Page 330 ~ Duplicate

Page 331 ~ Duplicate

Page 332 ~ Duplicate

Page 333 ~ Duplicate

THOMAS, JULIE F. (OGC) (FBI)

From: [redacted] (OCA) (FBI)
Sent: Thursday, February 17, 2005 11:24 AM
To: [redacted] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI)
Cc: [redacted] (OCA) (FBI); KELLEY, PATRICK W. (OGC) (FBI)
Subject: Request for Comments re: PATRIOT Act Sunsets Report

b6

b7C

UNCLASSIFIED**NON-RECORD**

b6

ALL INFORMATION CONTAINED

HEREIN IS UNCLASSIFIED

DATE 08-22-2005 BY 65179/DMH/JW/05-CV-0845

b7C

[redacted] and Julie:

DOJ's Office of Legislative Affairs (OLA) sent the attached draft report on the 16 provisions of the USA PATRIOT Act subject to sunset at the end of this year. The report was requested by the Senate Judiciary Subcmte on Terrorism and is meant to:

1. explain how these sixteen sections changed the legal landscape;
2. to survey and analyze the objections to these provisions lodged by opponents of the Act; and
3. to summarize how these sections of the Act have been used by the Department to protect the American people.

OLA has requested FBI comments on the report.

It is a lengthy report, so please focus on those sections in which you have expertise or interest. Feel free to read and comment on the entire document, but note there is a short time frame for review and OLA will not be able to give extensions.

I've copied Pat Kelley for his information and in the event he believes other OGC components should be asked to comment.

Please send comments to [redacted] ext. [redacted] by **9:00 am, Tuesday, 2/22/05.**

b2

b6

Thanks for your assistance.

b7C

[redacted]
Office of Congressional Affairs
JEH Building Room 7252
[redacted]

b2

b6

b7C

UNCLASSIFIED

6/15/2005

~~SECRET~~**THOMAS, JULIE F. (OGC) (FBI)**

From: [REDACTED] (OGC) (FBI) b6
Sent: Monday, March 28, 2005 4:45 PM b7C
To: THOMAS, JULIE F. (OGC) (FBI)
Subject: FW: Roving Authority

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Julie:

FYI. Just closing the loop to keep you informed. Valerie wanted to know the number of Roving FISAs done to date.

[REDACTED] b6 DATE: 08-22-2005
[REDACTED] b7C CLASSIFIED BY 65179/DMH/JW/05-CV-0845 ALL INFORMATION CONTAINED
REASON: 1.4 (C) HEREIN IS UNCLASSIFIED EXCEPT
DECLASSIFY ON: 08-22-2030 WHERE SHOWN OTHERWISE

-----Original Message-----

AAG

From: [REDACTED] (OGC) (OGA)
Sent: Monday, March 28, 2005 4:03 PM
To: [REDACTED] (OGC) (FBI)
Cc: [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI) b6
Subject: RE: Roving Authority b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[REDACTED] I just answered a similar question via an email from Valerie. The number of Section 206 orders since the b1
Patriot Act's signing to date is [REDACTED]. Does that give you what you need? Let me know if not, [REDACTED] b6
(S) b7C

-----Original Message-----

From: [REDACTED] (OGC) (FBI)
Sent: Monday, March 28, 2005 10:10 AM
To: [REDACTED] (OGC) (OGA)
Cc: [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI) b6
Subject: Roving Authority b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[REDACTED]

I am writing to follow up on a phone conversation I had with [REDACTED] last week before she left for vacation. Valerie Caproni has asked NSLB to determine how many times FISA Roving authority has been granted since the change in the law. [REDACTED] told me that you were compiling that information and other, similar, statistics. When you get the number, could please send it to us? b6

Thanks for your help. b7C

Best,

[REDACTED]

~~SECRET~~

6/15/2005

[REDACTED]
Assistant General Counsel
National Security Law Branch
FBIHQ Room 7975
Direct Line: [REDACTED]
Unclassified Fax: [REDACTED]
Secure Fax: [REDACTED]

b2
b6
b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

THOMAS, JULIE F. (OGC) (FBI)

From: [redacted] (OGC) (FBI) b6
Sent: Wednesday, March 16, 2005 2:15 PM b7C
To: [redacted] (OGC) (FBI)
Cc: THOMAS, JULIE F. (OGC) (FBI); [redacted] (OGC) (FBI) [redacted] (OGC) (FBI)
Subject: RE: 215, NSL etc

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
 HEREIN IS UNCLASSIFIED
 DATE 08-22-2005 BY 65179/DMH/JW/05-CV-0845

Which question(s) do you want me to answer? #1? #4?

[redacted]

b5

[redacted]

b5

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Wednesday, March 16, 2005 2:06 PM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Cc: THOMAS, JULIE F. (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: FW: 215, NSL etc

b6
 b7C

UNCLASSIFIED
NON-RECORD

[redacted]

I really need you to put this together.
 Let me know if you can meet this deadline.

[redacted]

b6
 b7C

Could you assist [redacted]

[redacted]

[redacted]

b6
 b7C

6/15/2005

THOMAS, JULIE F. (OGC) (FBI)

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Thursday, March 17, 2005 5:30 PM
To: Caproni, Valerie E. (OGC) (FBI)
Subject: RE: Patriot Act Examples

UNCLASSIFIED
NON-RECORD

yes.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-22-2005 BY 65179/DMH/JW/05-CV-0845

-----Original Message-----

From: Caproni, Valerie E. (OGC) (FBI)
Sent: Thursday, March 17, 2005 1:43 PM
To: THOMAS, JULIE F. (OGC) (FBI)
Subject: FW: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

Can you have the list of 215 orders ready by 3/25?

-----Original Message-----

From: KALISCH, ELENI P. (OCA) (FBI)
Sent: Thursday, March 17, 2005 12:07 PM
To: FBI_SAC's; FBI_ADs and EADs
Subject: Patriot Act Examples
Importance: High

UNCLASSIFIED
NON-RECORD

All:

As the Director mentioned at the SAC Conference earlier this week, 16 provisions of the Patriot Act are scheduled to "sunset" at the end of the year. In seeking reauthorization of these provisions, we need to provide Congress with examples of how these provisions have been helpful to us in all of our programs. The text of the Patriot Act, as well as a summary of the 16 "sunset" provisions, are located on the OCA intranet website under the "Legislation of Interest" link.

b2

Please review these provisions and submit unclassified examples to me via e-mail no later than Friday, March 25.

Although examples of all provisions are needed, of particular interest are examples of the following:

Sections 201 and 202 (Expanded Title III predicates)
Sections 203 and 218 (Information Sharing)
Section 206 (Roving Wiretaps)
Section 214 (FISA Pen Register and Trap/Trace)
Section 215 (Business Records)
Section 217 (Computer Hacking victims requesting law enforcement assistance)

Although not subject to sunset, Section 213 (Delayed Notice Search Warrants) remains controversial and

6/15/2005

examples of the utility of this provision are needed.

In your response, please identify a POC in your office in the event additional information is needed. Thank you for your assistance.

Eleni

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

THOMAS, JULIE F. (OGC) (FBI)**From:** THOMAS, JULIE F. (OGC) (FBI)**Sent:** Wednesday, March 16, 2005 11:35 AM**To:** [REDACTED] (OCA) (FBI)

b6

Cc: [REDACTED] (OGC) (FBI)

b7C

Subject: RE: DOJ Final Draft Report re Patriot Act Sunset Provisions**UNCLASSIFIED**
NON-RECORD

b6 , b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-22-2005 BY 65179/DMH/JW/05-CV-0845

Thanks [REDACTED] when do you need our comments, if any. Julie

-----Original Message-----

From: [REDACTED] (OCA) (FBI)

b6

Sent: Tuesday, March 15, 2005 6:51 PM

b7C

To: THOMAS, JULIE F. (OGC) (FBI); [REDACTED] (OGC) (FBI)**Subject:** DOJ Final Draft Report re Patriot Act Sunset Provisions**UNCLASSIFIED**
NON-RECORD

b6

Julie and [REDACTED] - attached is DOJ's final draft report to Senate Judiciary re the Patriot Act provisions scheduled to sunset. It's being circulated for final comments this week, with an anticipated dissemination date of 3/30/05. In the last go-around, NSLB didn't have any comments - but I wanted to give you an opportunity for a final look. If you could pay particular attention to the discussion of the FISA provisions, I would really appreciate it. Call if you have questions, Thanks,

b7C

[REDACTED]

b2

Office of Congressional Affairs

b6

[REDACTED]

b7C

UNCLASSIFIED**UNCLASSIFIED**

6/15/2005

THOMAS, JULIE F. (OGC) (FBI)

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Monday, February 21, 2005 2:51 PM
To: [REDACTED] (OGC) (FBI)
Subject: FW: Request for Comments re: PATRIOT Act Sunsets Report

b6

b7C

UNCLASSIFIED
NON-RECORD

Did I already forward this to you? Haven't we already commented on this once? Julie

-----Original Message-----

From: [REDACTED] (OCA) (FBI)
Sent: Thursday, February 17, 2005 11:24 AM
To: [REDACTED] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI)
Cc: [REDACTED] (OCA) (FBI); KELLEY, PATRICK W. (OGC) (FBI)
Subject: Request for Comments re: PATRIOT Act Sunsets Report

b6

b7C

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-22-2005 BY 65179/DMH/JW/05-CV-0845

b6

b7C

[REDACTED] and Julie:

DOJ's Office of Legislative Affairs (OLA) sent the attached draft report on the 16 provisions of the USA PATRIOT Act subject to sunset at the end of this year. The report was requested by the Senate Judiciary Subcommittee on Terrorism and is meant to:

1. explain how these sixteen sections changed the legal landscape;
2. to survey and analyze the objections to these provisions lodged by opponents of the Act; and
3. to summarize how these sections of the Act have been used by the Department to protect the American people.

OLA has requested FBI comments on the report.

It is a lengthy report, so please focus on those sections in which you have expertise or interest. Feel free to read and comment on the entire document, but note there is a short time frame for review and OLA will not be able to give extensions.

I've copied Pat Kelley for his information and in the event he believes other OGC components should be asked to comment.

Please send comments to [REDACTED] ext. [REDACTED] by **9:00 am, Tuesday, 2/22/05**.

b2

Thanks for your assistance.

b6

b7C

[REDACTED]
Office of Congressional Affairs
JEH Building Room 7252
[REDACTED]

b2

b6

b7C

UNCLASSIFIED

6/15/2005

UNCLASSIFIED

THOMAS, JULIE F. (OGC) (FBI)

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Tuesday, February 22, 2005 8:26 AM
To: [REDACTED] (OCA) (FBI)
Cc: [REDACTED] (OGC) (FBI); BEERS, ELIZABETH RAE (OCA) (FBI)
Subject: RE: Request for Comments re: PATRIOT Act Sunsets Report

b6

b7C

UNCLASSIFIED
NON-RECORD

I reviewed the attached legislation on behalf of NSLB and have no comments.

Julie Thomas

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-22-2005 BY 65179/DMH/JW/05-CV-0845

-----Original Message-----

From: [REDACTED] (OCA) (FBI)
Sent: Thursday, February 17, 2005 11:24 AM
To: [REDACTED] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI)
Cc: [REDACTED] (OCA) (FBI); KELLEY, PATRICK W. (OGC) (FBI)
Subject: Request for Comments re: PATRIOT Act Sunsets Report

b6

b7C

UNCLASSIFIED
NON-RECORD

b6

b7C

[REDACTED] and Julie:

DOJ's Office of Legislative Affairs (OLA) sent the attached draft report on the 16 provisions of the USA PATRIOT Act subject to sunset at the end of this year. The report was requested by the Senate Judiciary Subcommittee on Terrorism and is meant to:

1. explain how these sixteen sections changed the legal landscape;
2. to survey and analyze the objections to these provisions lodged by opponents of the Act; and
3. to summarize how these sections of the Act have been used by the Department to protect the American people.

OLA has requested FBI comments on the report.

It is a lengthy report, so please focus on those sections in which you have expertise or interest. Feel free to read and comment on the entire document, but note there is a short time frame for review and OLA will not be able to give extensions.

I've copied Pat Kelley for his information and in the event he believes other OGC components should be asked to comment.

Please send comments to [REDACTED] ext. [REDACTED] by **9:00 am, Tuesday, 2/22/05**.

b2

Thanks for your assistance.

b6

b7C

[REDACTED]
Office of Congressional Affairs
JEH Building Room 7252

b2

b6

b7C

6/15/2005

UNCLASSIFIED

UNCLASSIFIED

THOMAS, JULIE F. (OGC) (FBI)

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Friday, February 11, 2005 5:47 PM
To: [REDACTED] (OCA) (FBI)
Subject: RE: NSLB Review of DOJ Draft Legislation

b6

b7C

UNCLASSIFIED
NON-RECORD

It will be me. Thanks, Julie

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-22-2005 BY 65179/DMH/JW/05-CV-0845

-----Original Message-----

From: [REDACTED] (OCA) (FBI)
Sent: Friday, February 11, 2005 5:46 PM
To: THOMAS, JULIE F. (OGC) (FBI)
Subject: NSLB Review of DOJ Draft Legislation

b6

b7C

UNCLASSIFIED
NON-RECORD

Julie - reference our conversation yesterday concerning the need to identify an NSLB attorney to assist with review of DOJ material in connection with efforts relating to the USA Patriot Act reauthorization. I have copies of 4 drafts circulated by DOJ for component comment. I need NSLB's comments by noon on 2/18/2005 to meet DOJ's deadline. As I mentioned on the phone, DOJ considers this material extremely sensitive and has instructed us to limit dissemination. Please identify an NSLB point of contact and I will deliver the material. Thanks,

[REDACTED]

Office of Congressional Affairs

[REDACTED]

b2

b6

b7C

UNCLASSIFIED

UNCLASSIFIED

6/15/2005

THOMAS, JULIE F. (OGC) (FBI)

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Wednesday, January 19, 2005 1:49 PM
To: [REDACTED] (OGC) (OGA)
Cc: [REDACTED] (OCA) (FBI)
Subject: RE: sunset

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
 HEREIN IS UNCLASSIFIED
 DATE 08-22-2005 BY 65179/DMH/JW/05-CV-0845

Great. [REDACTED] let me know if you need anything else from us. Julie

b6
b7C

-----Original Message-----

From: [REDACTED] (OGC) (OGA)
Sent: Wednesday, January 19, 2005 1:46 PM
To: THOMAS, JULIE F. (OGC) (FBI)
Cc: [REDACTED] (OCA) (FBI)
Subject: sunset

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Julie:

[REDACTED] and I just spoke and agreed that we would take out the sublist of USA Patriot Act provisions that will sunset and just refer to them generally. [REDACTED] will send DOJ our comments concerning the significant purpose standard in FISA.

b6
b7C

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

6/15/2005

THOMAS, JULIE F. (OGC) (FBI)

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Wednesday, December 15, 2004 3:13 PM
To: [REDACTED] (OGC) (FBI)
Cc: [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI)
Subject: RE: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
 HEREIN IS UNCLASSIFIED
 DATE 08-22-2005 BY 65179/DMH/JW/05-CV-0845

So, [REDACTED] will you put together a sample letter with an EC to the field regarding its use for our approval and dissemination? Thanks, Julie

b6
b7C

-----Original Message-----

From: [REDACTED] (OGC) (FBI)
Sent: Tuesday, December 14, 2004 11:16 AM
To: [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); [REDACTED] (ITD)
 (FBI); THOMAS, JULIE F. (OGC) (FBI); KELLEY, PATRICK W. (OGC) (FBI); [REDACTED] (OGC) (FBI);
 [REDACTED] (OGC) (FBI)
Subject: RE: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

[REDACTED]

b5

[REDACTED]

b5

[REDACTED]

b5

[REDACTED]

b5

[Redacted]

b5

[Redacted]

b5

[Redacted]

b5

[Redacted]

[Redacted] I think it is a good idea for OGC to review these requests before they go out to ensure compliance with 2702, since the facts will change in each case. Thanks. Dan

b5

-----Original Message-----

From: [Redacted] (OGC) (FBI)
Sent: Friday, December 10, 2004 9:45 AM
To: [Redacted] (OGC) (FBI)
Subject: FW: 207208 letter

b6

b7C

UNCLASSIFIED
NON-RECORD

FYI

-----Original Message-----

From: [Redacted] (ITD) (FBI)
Sent: Monday, November 15, 2004 8:05 PM
To: [Redacted] (OGC) (FBI); [Redacted] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI); KELLEY, PATRICK W. (OGC) (FBI)
Cc: [Redacted] (ITD) (FBI)
Subject: RE: 207208 letter

b6

b7C

UNCLASSIFIED
NON-RECORD

Unless I hear back otherwise, given everyone's comments, I will reply back to the USAO that FBI OGC is reviewing the matter and that they should inform the local FBI agents that they should not send out the letter without first conferring with FBI OGC NSLB.

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI
 WITHOUT PRIOR OGC APPROVAL

[Redacted]

Science & Technology Law Unit
 Engineering Research Facility
 Bldg 27958A, Room A-207
 Quantico, VA 22135
 Tel. [Redacted]
 Fax [Redacted]

b2

b6

b7C

-----Original Message-----

6/15/2005

From: [redacted] (OGC) (FBI)
Sent: Monday, November 15, 2004 11:43 AM
To: [redacted] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI); [redacted]
 (ITD) (FBI)
Subject: RE: 207208 letter

b6
 b7C

UNCLASSIFIED
NON-RECORD

Since the pony [redacted] sent refers to ITOS II, let me see what I can find out from my end.

b6
 b7C

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Monday, November 15, 2004 10:46 AM
To: THOMAS, JULIE F. (OGC) (FBI); [redacted] (OGC) (FBI); [redacted]
 [redacted] (ITD) (FBI)
Subject: FW: 207208 letter

b6
 b7C

UNCLASSIFIED
NON-RECORD

[redacted] comments.

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Monday, November 15, 2004 10:35 AM
To: [redacted] (OGC) (FBI)
Subject: RE: 207208 letter

b6
 b7C

UNCLASSIFIED
NON-RECORD

I have never seen this. I agree with [redacted]

[redacted]

b5
 b6
 b7C

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Monday, November 15, 2004 9:10 AM
To: [redacted] (OGC) (FBI)
Subject: FW: 207208 letter

b6
 b7C

UNCLASSIFIED
NON-RECORD

What do you think?

-----Original Message-----

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Monday, November 15, 2004 8:36 AM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: FW: 207208 letter

UNCLASSIFIED

b6
 b7C

NON-RECORD

Dear [redacted] and [redacted]

b6

b7C

Please note the attachments from [redacted] Is this letter one we have approved ? Please advise,

Julie

-----Original Message-----

b6

From: [redacted] (ITD) (FBI)

b7C

Sent: Friday, November 12, 2004 4:01 PM

To: THOMAS, JULIE F. (OGC) (FBI)

Cc: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI);

KELLEY, PATRICK W. (OGC) (FBI); [redacted] (ITD) (FBI); [redacted]

Steven (OGC) (FBI)

Subject: FW: 207208 letter

UNCLASSIFIED

NON-RECORD

Attached is a copy of a form letter sent to me via one of the U.S. Attorney's Offices [redacted]



b5

Is this an OGC/NSLB approved letter?

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE
OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

[redacted]

Science & Technology Law Unit

b2

Engineering Research Facility

b6

Bldg 27958A, Room A-207

Quantico, VA 22135

b7C

Tel [redacted]
Fax [redacted]

-----Original Message-----

From: [redacted] (ITOD)(CON)

b6

Sent: Friday, November 12, 2004 8:59 AM

To: [redacted] (ITD) (FBI)

b7C

6/15/2005

Subject: 207208 letter

UNCLASSIFIED
NON-RECORD

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

6/15/2005

THOMAS, JULIE F. (OGC) (FBI)

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Tuesday, November 16, 2004 12:35 PM
To: [REDACTED] (ITD) (FBI)
Subject: RE: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 08-22-2005 BY 65179/DMH/JW/05-CV-0845

Sounds good. Julie

-----Original Message-----

From: [REDACTED] (ITD) (FBI)
Sent: Monday, November 15, 2004 8:05 PM
To: [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI);
[REDACTED] (OGC) (FBI)
Cc: [REDACTED] (ITD) (FBI)
Subject: RE: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

Unless I hear back otherwise, given everyone's comments, I will reply back to the USAO that FBI OGC is reviewing the matter and that they should inform the local FBI agents that they should not send out the letter without first conferring with FBI OGC NSLB.

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT
PRIOR OGC APPROVAL

[REDACTED]
Science & Technology Law Unit
Engineering Research Facility
Bldg 27958A, Room A-207
Quantico, VA 22135
Tel. [REDACTED]
Fax. [REDACTED]

b2
b6
b7C

-----Original Message-----

From: [REDACTED] (OGC) (FBI)
Sent: Monday, November 15, 2004 11:43 AM
To: [REDACTED] (OGC) (FBI); THOMAS, JULIE F. (OGC) (FBI); [REDACTED] (ITD)
(FBI)
Subject: RE: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

Since the pony [REDACTED] sent refers to ITOS II, let me see what I can find out from my end.

b6
b7C

6/15/2005

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Monday, November 15, 2004 10:46 AM
To: THOMAS, JULIE F. (OGC) (FBI); [redacted] (OGC) (FBI); [redacted] (ITD) (FBI)
Subject: FW: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] comments.

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Monday, November 15, 2004 10:35 AM
To: [redacted] (OGC) (FBI)
Subject: RE: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

I have never seen this. I agree with [redacted]

b5
b6
b7C

-----Original Message-----

From: [redacted] (OGC) (FBI)
Sent: Monday, November 15, 2004 9:10 AM
To: [redacted] (OGC) (FBI)
Subject: FW: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

What do you think?

-----Original Message-----

From: THOMAS, JULIE F. (OGC) (FBI)
Sent: Monday, November 15, 2004 8:36 AM
To: [redacted] (OGC) (FBI); [redacted] (OGC) (FBI)
Subject: FW: 207208 letter

b6
b7C

UNCLASSIFIED
NON-RECORD

Dear [redacted] and [redacted]

Please note the attachments from [redacted] Is this letter one we have approved and if so, are [redacted] concerns valid? Please advise,

b6
b7C

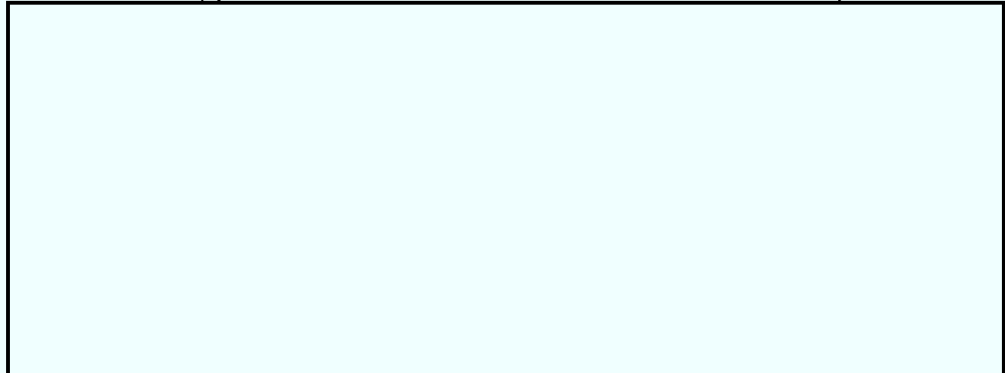
Julie

-----Original Message-----

From: [REDACTED] (ITD) (FBI) b6
Sent: Friday, November 12, 2004 4:01 PM b7C
To: THOMAS, JULIE F. (OGC) (FBI)
Cc: [REDACTED] (OGC) (FBI); [REDACTED] (OGC) (FBI); KELLEY, PATRICK W. (OGC) (FBI); [REDACTED] (ITD) (FBI); [REDACTED] (OGC) (FBI)
Subject: FW: 207208 letter

UNCLASSIFIED
NON-RECORD

Attached is a copy of a form letter sent to me via one of the U.S. Attorney's Offices.



b5

Is this an OGC/NSLB approved letter?

PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL



Science & Technology Law Unit
 Engineering Research Facility
 Bldg 27958A, Room A-207
 Quantico, VA 22135
 Tel. [REDACTED]
 Fax [REDACTED]

b2
 b6
 b7C

-----Original Message-----

From: [REDACTED] (ITOD)(CON) b6
Sent: Friday, November 12, 2004 8:59 AM b7C
To: [REDACTED] (ITD) (FBI)
Subject: 207208 letter

UNCLASSIFIED
NON-RECORD

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED